

SPLK-1002 Dumps

Splunk Core Certified Power User Exam

<https://www.certleader.com/SPLK-1002-dumps.html>



NEW QUESTION 1

- (Exam Topic 1)

A space is an implied _____ in a search string.

- A. OR
- B. AND
- C. ()
- D. NOT

Answer: B

Explanation:

A space is an implied AND in a search string, which means that it acts as a logical operator that returns events that match both terms on either side of the space². For example, status=200 method=GET will return event that have both status=200 and method=GET². Therefore, option B is correct, while options A, C and D are incorrect because they are not implied by a space in a search string.

NEW QUESTION 2

- (Exam Topic 1)

Which of the following statements about tags is true?

- A. Tags are case insensitive.
- B. Tags are created at index time.
- C. Tags can make your data more understandable.
- D. Tags are searched by using the syntax tag: : <fieldneme>

Answer: C

Explanation:

Tags are aliases or alternative names for field values in Splunk. They can make your data more understandable by using common or descriptive terms instead of cryptic or technical terms. For example, you can tag a field value such as “200” with “OK” or “success” to indicate that it is a HTTP status code for a successful request. Tags are case sensitive, meaning that “OK” and “ok” are different tags. Tags are created at search time, meaning that they are applied when you run a search on your data. Tags are searched by using the syntax tag::<tagname>, where <tagname> is the name of the tag you want to search for.

NEW QUESTION 3

- (Exam Topic 1)

Which of the following knowledge objects represents the output of an eval expression?

- A. Eval fields
- B. Calculated fields
- C. Field extractions
- D. Calculated lookups

Answer: B

Explanation:

Reference: <https://docs.splunk.com/Splexicon:Calculatedfield>

The eval command is used to create new fields or modify existing fields based on an expression². The output of an eval expression is a calculated field, which is a field that you create based on the value of another field or fields². You can use calculated fields to enrich your data with additional information or to transform your data into a more useful format². Therefore, option B is correct, while options A, C and D are incorrect because they are not names of knowledge objects that represent the output of an eval expression.

NEW QUESTION 4

- (Exam Topic 1)

How does a user display a chart in stack mode?

- A. By using the stack command.
- B. By turning on the Use Trellis Layout option.
- C. By changing Stack Mode in the Format menu.
- D. You cannot display a chart in stack mode, only a timechart.

Answer: C

Explanation:

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. Sta 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.

NEW QUESTION 5

- (Exam Topic 1)

Which group of users would most likely use pivots?

- A. Users
- B. Architects
- C. Administrators
- D. Knowledge Managers

Answer:

A

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Pivot/IntroductiontoPivot>

A pivot is a tool that allows you to create reports and dashboards using data models without writing any SPL commands². You can use pivots to explore, filter, split and visualize your data using a graphical interface². Pivots are designed for users who want to analyze and report on their data without having to learn the SPL syntax or the underlying structure of the data². Therefore, option A is correct, while options B, C and D are incorrect because they are not the typical group of users who would use pivots.

NEW QUESTION 6

- (Exam Topic 1)

Given the macro definition below, what should be entered into the Name and Arguments fields to correctly configured the macro?

Destination app
oidemo

Name *
Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to

Definition *
Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them

```
sourcetype=access_combined action=$action$ JSESSIONID=$JSESSIONID$ | stats values(action) as action by JSESSIONID
```

☐ Use eval-based definition?

Arguments
Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.

- A. The macro name is sessiontracker and the arguments are action, JSESSIONID.
- B. The macro name is sessiontracker(2) and the arguments are action, JSESSIONID.
- C. The macro name is sessiontracker and the arguments are \$action\$, \$JSESSIONID\$.
- D. The macro name is sessiontracker(2) and the Arguments are \$action\$, \$JSESSIONID\$.

Answer: B

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Definesearchmacros>

The macro definition below shows a macro that tracks user sessions based on two arguments: action and JSESSIONID.

sessiontracker(2)

The macro definition does the following:

It specifies the name of the macro as sessiontracker. This is the name that will be used to execute the macro in a search string.

It specifies the number of arguments for the macro as 2. This indicates that the macro takes two arguments when it is executed.

It specifies the code for the macro as `index=main sourcetype=access_combined_wcookie action=$action$ JSESSIONID=$JSESSIONID$ | stats count by JSESSIONID`. This is the search string that will be run when the macro is executed. The search string can contain any part of a search, such as search terms, commands, arguments, etc. The search string can also include variables for the arguments using dollar signs around them. In this case, action and JSESSIONID are variables for the arguments that will be replaced by their values when the macro is executed.

Therefore, to correctly configure the macro, you should enter sessiontracker as the name and action, JSESSIONID as the arguments. Alternatively, you can use sessiontracker(2) as the name and leave the arguments blank.

NEW QUESTION 7

- (Exam Topic 1)

Calculated fields can be based on which of the following?

- A. Tags
- B. Extracted fields
- C. Output fields for a lookup
- D. Fields generated from a search string

Answer: B

Explanation:

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

A calculated field is a field that you create based on the value of another field or fields¹. You can use calculated fields to enrich your data with additional information or to transform your data into a more useful format¹. Calculated fields can be based on extracted fields, which are fields that are extracted from your raw data using various methods such as regular expressions, delimiters, or key-value pairs¹. Therefore, option B is correct, while options A, C and D are incorrect because tags, output fields for a lookup, and fields generated from a search string are not types of extracted fields.

NEW QUESTION 8

- (Exam Topic 1)

Selected fields are displayed _____ each event in the search results.

- A. below
- B. interesting fields
- C. other fields
- D. above

Answer: A

Explanation:

Selected fields are fields that you choose to display in your search results by clicking on them in the Fields sidebar or by using the fields command². Selected fields are displayed below each event in the search results, along with their values². Therefore, option A is correct, while options B, C and D are incorrect because they are not places where selected fields are displayed.

NEW QUESTION 9

- (Exam Topic 1)

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?

- A. Both will appear in the All Fields list, but only if the alias is specified in the search.
- B. Both will appear in the Interesting Fields list, but only if they appear in at least 20 percent of events.
- C. The original field only appears in All Fields list and the alias only appears in the Interesting Fields list.
- D. The alias only appears in the All Fields list and the original field only appears in the Interesting Fields list.

Answer: B

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 10

- (Exam Topic 1)

Which of the following data model are included In the Splunk Common Information Model (CIM) add-on? (select all that apply)

- A. Alerts
- B. Email
- C. Database
- D. User permissions

Answer: ABC

Explanation:

Reference: <https://docs.splunk.com/Documentation/CIM/4.15.0/User/Overview>

The Splunk Common Information Model (CIM) add-on is a collection of pre-built data models and knowledge objects that help you normalize your data from different sources and make it easier to analyze and report on it³. The CIM add-on includes several data models that cover various domains such as Alerts, Email, Database, Network Traffic, Web and more³. Therefore, options A, B and C are correct because they are names of some of the data models included in the CIM add-on. Option D is incorrect because User permissions is not a name of a data model in the CIM add-on.

NEW QUESTION 10

- (Exam Topic 1)

Which of the following statements describe the search below? (select all that apply) `Index=main | transaction clientip host maxspan=30s maxpause=5s`

- A. Events in the transaction occurred within 5 seconds.
- B. It groups events that share the same clientip and host.
- C. The first and last events are no more than 5 seconds apart.
- D. The first and last events are no more than 30 seconds apart.

Answer: ABD

Explanation:

The search below groups events by two or more fields (clientip and host), creates transactions with start and end constraints (maxspan=30s and maxpause=5s), and calculates the duration of each transaction.

`index=main | transaction clientip host maxspan=30s maxpause=5s` The search does the following:

- It filters the events by the index main, which is a default index in Splunk that contains all data that is not sent to other indexes.
- It uses the transaction command to group events into transactions based on two fields: clientip and host.

The transaction command creates new events from groups of events that share the same clientip and host values.

- It specifies the start and end constraints for the transactions using the maxspan and maxpause arguments. The maxspan argument sets the maximum time span between the first and last events in a transaction. The maxpause argument sets the maximum time span between any two consecutive events in a transaction. In this case, the maxspan is 30 seconds and the maxpause is 5 seconds, meaning that any transaction that has a longer time span or pause will be split into multiple transactions.

- It creates some additional fields for each transaction, such as duration, eventcount, starttime, etc. The duration field shows the time span between the first and last events in a transaction.

NEW QUESTION 14

- (Exam Topic 1)

When performing a regular expression (regex) field extraction using the Field Extractor (FX), what happens when the require option is used?

- A. The regex can no longer be edited.
- B. The field being extracted will be required for all future events.
- C. The events without the required field will not display in searches.
- D. Only events with the required string will be included in the extraction.

Answer: D

Explanation:

The Field Extractor (FX) allows you to use regular expressions (regex) to extract fields from your events using a graphical interface or by manually editing the regex2. When you use the FX to perform a regex field extraction, you can use the require option to specify a string that must be present in an event for it to be included in the extraction2. This way, you can filter out events that do not contain the required string and focus on the events that are relevant for your extraction2. Therefore, option D is correct, while options A, B and C are incorrect.

NEW QUESTION 16

- (Exam Topic 1)

Which of the following eval command function is valid?

- A. Int ()
- B. Count ()
- C. Print ()
- D. ToString ()

Answer: D

Explanation:

The eval command supports a number of functions that you can use in your expressions to perform calculations, conversions, string manipulations and more2. One of the eval command functions is tostring(), which converts a numeric value to a string value2. Therefore, option D is correct, while options A, B and C are incorrect because they are not valid eval command functions.

NEW QUESTION 20

- (Exam Topic 1)

What are the two parts of a root event dataset?

- A. Fields and variables.
- B. Fields and attributes.
- C. Constraints and fields.
- D. Constraints and lookups.

Answer: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/SplunkLight/7.3.5/GettingStarted/Designadatamodelobjects> A root event dataset is the base dataset for a data model that defines the source or sources of the data and the constraints and fields that apply to the data1. A root event dataset has two parts: constraints and fields1. Constraints are filters that limit the data to a specific index, source, sourcetype, host or search string1. Fields are the attributes that describe the data and can be extracted, calculated or looked up1. Therefore, option C is correct, while options A, B and D are incorrect.

NEW QUESTION 24

- (Exam Topic 1)

Which of the following statements about event types is true? (select all that apply)

- A. Event types can be tagged.
- B. Event types must include a time range,
- C. Event types categorize events based on a search.
- D. Event types can be a useful method for capturing and sharing knowledge.

Answer: ACD

Explanation:

Reference: <https://www.edureka.co/blog/splunk-events-event-types-and-tags/>

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.

NEW QUESTION 25

- (Exam Topic 1)

Which of the following file formats can be extracted using a delimiter field extraction?

- A. CSV
- B. PDF
- C. XML
- D. JSON

Answer: A

Explanation:

A delimiter field extraction is a method of extracting fields from data that uses a character or a string to separate fields in each event. A delimiter field extraction can be performed by using the Field Extractor (FX) tool or by editing the props.conf file. A delimiter field extraction can be applied to any file format that uses a delimiter to separate fields, such as CSV, TSV, PSV, etc. A CSV file is a comma-separated values file that uses commas as delimiters. Therefore, a CSV file can be extracted using a delimiter field extraction.

NEW QUESTION 27

- (Exam Topic 1)

Which of the following statements describe calculated fields? (select all that apply)

- A. Calculated fields can be used in the search bar.
- B. Calculated fields can be based on an extracted field.
- C. Calculated fields can only be applied to host and sourcetype.
- D. Calculated fields are shortcuts for performing calculations using the eval command.

Answer: ABD

Explanation:

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.

NEW QUESTION 31

- (Exam Topic 2)

Which of the following about reports is/are true?

- A. Reports are knowledge objects.
- B. Reports can be scheduled.
- C. Reports can run a script.
- D. All of the above.

Answer: D

Explanation:

A report is a way to save a search and its results in a format that you can reuse and share with others². A report is also a type of knowledge object, which is an entity that you create to add knowledge to your data and make it easier to search and analyze². Therefore, option A is correct. A report can be scheduled, which means that you can configure it to run at regular intervals and send the results to yourself or others via email or other methods². Therefore, option B is correct. A report can run a script, which means that you can specify a script file to execute when the report runs and use it to perform custom actions or integrations². Therefore, option C is correct. Therefore, option D is correct because all of the above statements are true for reports.

NEW QUESTION 35

- (Exam Topic 2)

Which of the following search modes automatically returns all extracted fields in the fields sidebar?

- A. Fast
- B. Smart
- C. Verbose

Answer: C

Explanation:

The search modes determine how Splunk processes your search and displays your results². There are three search modes: Fast, Smart and Verbose². The search mode that automatically returns all extracted fields in the fields sidebar is Verbose². The Verbose mode shows all the fields that are extracted from your events, including default fields, indexed fields and search-time extracted fields². The fields sidebar is a panel that shows the fields that are present in your search results². Therefore, option C is correct, while options A and B are incorrect because they are not search modes that automatically return all extracted fields in the fields sidebar.

NEW QUESTION 36

- (Exam Topic 2)

Which of the following searches will show the number of categoryId used by each host?

- A. Sourcetype=access_* |sum bytes by host
- B. Sourcetype=access_* |stats sum(categoryId) by host
- C. by host
- D. Sourcetype=access_* |sum(bytes) by host
- E. Sourcetype=access_* |stats sum by host

Answer: B

NEW QUESTION 40

- (Exam Topic 2)

What approach is recommended when using the Splunk Common Information Model (CIM) add-on to normalize data?

- A. Consult the CIM data model reference tables.
- B. Run a search using the authentication command.
- C. Consult the CIM event type reference tables.
- D. Run a search using the correlation command.

Answer: A

Explanation:

The recommended approach when using the Splunk Common Information Model (CIM) add-on to normalize data is A. Consult the CIM data model reference tables. This is because the CIM data model reference tables provide detailed information about the fields and tags that are expected for each dataset in a data model. By consulting the reference tables, you can determine which data models are relevant for your data source and how to map your data fields to the CIM fields. You can also use the reference tables to validate your data and troubleshoot any issues with normalization. You can find the CIM data model reference tables in the Splunk documentation¹ or in the Data Model Editor page in Splunk Web². The other options are incorrect because they are not related to the CIM add-on or data normalization. The authentication command is a custom command that validates events against the Authentication data model, but it does not help you to normalize other types of data. The correlation command is a search command that performs statistical analysis on event fields, but it does not help you to map your data fields to the CIM fields. The CIM event type reference tables do not exist, as event types are not part of the CIM add-on.

NEW QUESTION 42

- (Exam Topic 2)

The eval command 'if' function requires the following three arguments (in order):

- A. Boolean expression, result if true, result if false
- B. Result if true, result if false, boolean expression
- C. Result if false, result if true, boolean expression
- D. Boolean expression, result if false, result if true

Answer: A

Explanation:

The eval command 'if' function requires the following three arguments (in order): boolean expression, result if true, result if false. The eval command is a search command that allows you to create new fields or modify existing fields by performing calculations or transformations on them. The eval command can use various functions to perform different operations on fields. The 'if' function is one of the functions that can be used with the eval command to perform conditional evaluations on fields. The 'if' function takes three arguments: a boolean expression that evaluates to true or false, a result that will be returned if the boolean expression is true, and a result that will be returned if the boolean expression is false. The 'if' function returns one of the two results based on the evaluation of the boolean expression.

NEW QUESTION 47

- (Exam Topic 2)

What are the expected results for a search that contains the command | where A=B?

- A. Events that contain the string value where A=B.
- B. Events that contain the string value A=B.
- C. Events where values of field are equal to values of field B.
- D. Events where field A contains the string value B.

Answer: C

Explanation:

The correct answer is C. Events where values of field A are equal to values of field B.

The where command is used to filter the search results based on an expression that evaluates to true or false. The where command can compare two fields, two values, or a field and a value. The where command can also use functions, operators, and wildcards to create complex expressions¹.

The syntax for the where command is:

| where <expression>

The expression can be a comparison, a calculation, a logical operation, or a combination of these. The expression must evaluate to true or false for each event.

To compare two fields with the where command, you need to use the field names without any quotation marks. For example, if you want to find events where the values for the field A match the values for the field

B, you can use the following syntax:

| where A=B

This will return only the events where the two fields have the same value.

The other options are not correct because they use different syntax or fields that are not related to the where command. These options are:

- A. Events that contain the string value where A=B: This option uses the string value where A=B as a search term, which is not valid syntax for the where command. This option will return events that have the literal text "where A=B" in them.
- B. Events that contain the string value A=B: This option uses the string value A=B as a search term, which is not valid syntax for the where command. This option will return events that have the literal text "A=B" in them.
- D. Events where field A contains the string value B: This option uses quotation marks around the value B, which is not valid syntax for comparing fields with the where command. Quotation marks are used to enclose phrases or exact matches in a search². This option will return events where the field A contains the string value "B".

References:

- [where command usage](#)
- [Search command cheatsheet](#)

NEW QUESTION 51

- (Exam Topic 2)

When using the timechart command, how can a user group the events into buckets based on time?

- A. Using the span argument.
- B. Using the duration argument.
- C. Using the interval argument.

D. Adjusting the fieldformat options.

Answer: A

NEW QUESTION 56

- (Exam Topic 2)

Which syntax is used to represent an argument in a macro definition?

- A. "argument"
- B. %argument%
- C. 'argument'
- D. \$argument\$

Answer: D

Explanation:

The correct answer is D.

A search macro is a way to reuse a piece of SPL code in different searches. A search macro can take arguments, which are variables that can be replaced by different values when the macro is called. A search macro can also contain another search macro within it, which is called a nested macro1.

To represent an argument in a macro definition, you need to use the dollar sign (\$) character to enclose the argument name. For example, if you want to create a search macro that takes one argument named "object", you can use the following syntax:

```
[my_macro(object)] search sourcetype= object
```

This will create a search macro named my_macro that takes one argument named object. When you call the macro in a search, you need to provide a value for the object argument, such as:

```
my_macro(web)
```

This will replace the object argument with the value web and run the following SPL code: search sourcetype=web

The other options are not correct because they use quotation marks (' or ") or percentage signs (%) to represent arguments, which are not valid syntax for macro arguments. These characters will be interpreted as literal values instead of variables.

References:

➤ [Use search macros in searches](#)

NEW QUESTION 58

- (Exam Topic 2)

Information needed to create a GET workflow action includes which of the following? (select all that apply.)

- A. A name of the workflow action
- B. A URI where the user will be directed at search time.
- C. A label that will appear in the Event Action menu at search time.
- D. A name for the URI where the user will be directed at search time.

Answer: ABC

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/SetupaGETworkflowaction> Information needed to create a GET workflow action includes the following: a name of the workflow action, a URI where the user will be directed at search time, and a label that will appear in the Event Action menu at search time. A GET workflow action is a type of workflow action that performs a GET request when you click on a field value in your search results. A GET workflow action can be configured with various options, such as:

A name of the workflow action: This is a unique identifier for the workflow action that is used internally by Splunk. The name should be descriptive and meaningful for the purpose of the workflow action.

A URI where the user will be directed at search time: This is the base URL of the external web service or application that will receive the GET request. The URI can include field value variables that will be replaced by the actual field values at search time. For example, if you have a field value variable ip, you can write it as [http://example.com/ip=\\$ip](http://example.com/ip=$ip) to send the IP address as a parameter to the external web service or application.

A label that will appear in the Event Action menu at search time: This is the display name of the workflow action that will be shown in the Event Action menu when you click on a field value in your search results. The label should be clear and concise for the user to understand what the workflow action does.

Therefore, options A, B, and C are correct.

NEW QUESTION 61

- (Exam Topic 2)

The macro weekly_sales (2) contains the search string:

index—games l eval Product Sales = \$price\$ \$AmountS01d\$ Which of the following will return results?

- A. 'weekly_sales(3.99, 10) '
- B. 'weekly_sales(\$3.99\$, \$10\$)
- C. 'weekly_sales (3.99, 10)
- D. 'weekly_sales(3)

Answer: C

Explanation:

The correct answer is C. 'weekly_sales (3.99, 10)'. This is because search macros accept arguments without quotation marks or dollar signs, and the number of arguments must match the number of parameters defined in the macro. The other options are incorrect because they either use quotation marks or dollar signs around the arguments, or they provide a different number of arguments than the macro expects. You can learn more about how to use search macros in searches from the Splunk documentation1.

NEW QUESTION 66

- (Exam Topic 2)

How are event types different from saved reports?

- A. Event types cannot be used to organize data into categories.
- B. Event types include formatting of the search results.
- C. Event types can be shared with Splunk users and added to dashboards.
- D. Event types do not include a time range.

Answer: D

Explanation:

Hello, this is Bing. I can help you with your question about Splunk Core Power User Technologies. The correct answer is D. Event types do not include a time range.

The explanation is as follows:

- Event types are a categorization system that help you make sense of your data by matching events with the same search string¹. Event types are applied to events at search time and can be used as search terms or filters².
- Saved reports are results saved from a search action that can show statistics and visualizations of events³. Saved reports can be run anytime, and they fetch fresh results each time they are run³⁴. Saved reports can be shared with other users and added to dashboards⁴.
- The main difference between event types and saved reports is that event types do not include a time range, while saved reports do¹⁴. This means that event types can match events from any time period, while saved reports are limited by the time range specified when they are created or run¹⁴.

NEW QUESTION 68

- (Exam Topic 2)

Which workflow action method can be used the action type is set to link?

- A. GET
- B. PUT
- C. Search
- D. UPDATE

Answer: A

Explanation:

<https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/SetupaGETworkflowaction>

Define a GET workflow action

Steps

- Navigate to Settings > Fields > Workflow Actions.
- Click New to open up a new workflow action form.
- Define a Label for the action.

The Label field enables you to define the text that is displayed in either the field or event workflow menu.

Labels can be static or include the value of relevant fields.

- Determine whether the workflow action applies to specific fields or event types in your data.

Use Apply only to the following fields to identify one or more fields. When you identify fields, the workflow

action only appears for events that have those fields, either in their event menu or field menus. If you leave it blank or enter an asterisk the action appears in menus for all fields.

Use Apply only to the following event types to identify one or more event types. If you identify an event

type, the workflow action only appears in the event menus for events that belong to the event type.

- For Show action in determine whether you want the action to appear in the Event menu, the Fields menus, or Both.
- Set Action type to link.
- In URI provide a URI for the location of the external resource that you want to send your field values to.

Similar to the Label setting, when you declare the value of a field, you use the name of the field enclosed by dollar signs.

Variables passed in GET actions via URIs are automatically URL encoded during transmission. This means you can include values that have spaces between words or punctuation characters.

- Under Open link in, determine whether the workflow action displays in the current window or if it opens the link in a new window.
- Set the Link method to get.
- Click Save

to save your workflow action definition.

NEW QUESTION 69

- (Exam Topic 2)

What happens when a user edits the regular expression (regex) field extraction generated in the Field Extractor (FX)?

- A. There is a limit to the number of fields that can be extracted.
- B. The user is unable to preview the extractions.
- C. The extraction is added at index time.
- D. The user is unable to return to the automatic field extraction workflow.

Answer: A

NEW QUESTION 72

- (Exam Topic 2)

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

SEARCH: sourcetype=access* |fields action productId status

- A. is looking for all events that include the search terms: fields AND action AND productId AND status
- B. users the table command to improve performance

- C. limits the fields are extracted
- D. returns a table with 3 columns

Answer: C

NEW QUESTION 76

- (Exam Topic 2)

Which type of workflow action sends field values to an external resource (e.g. a ticketing system)?

- A. POST
- B. Search
- C. GET
- D. Format

Answer: A

Explanation:

The type of workflow action that sends field values to an external resource (e.g. a ticketing system) is POST. A POST workflow action allows you to send a POST request to a URI location with field values or static values as arguments. For example, you can use a POST workflow action to create a ticket in an external system with information from an event.

NEW QUESTION 77

- (Exam Topic 2)

When should transaction be used?

- A. Only in a large distributed Splunk environment.
- B. When calculating results from one or more fields.
- C. When event grouping is based on start/end values.
- D. When grouping events results in over 1000 events in each group.

Answer: C

NEW QUESTION 80

- (Exam Topic 2)

In the Field Extractor, when would the regular expression method be used?

- A. When events contain JSON data.
- B. When events contain comma-separated data.
- C. When events contain unstructured data.
- D. When events contain table-based data.

Answer: C

Explanation:

The correct answer is C. When events contain unstructured data.

The regular expression method works best with unstructured event data, such as log files or text messages, where the fields are not separated by a common delimiter, such as a comma or space¹. You select a sample event and highlight one or more fields to extract from that event, and the field extractor generates a regular expression that matches similar events in your dataset and extracts the fields from them¹. The regular expression method provides several tools for testing and refining the accuracy of the regular expression. It also allows you to manually edit the regular expression¹.

The delimiters 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 or space¹. You select a sample event, identify the delimiter, and then rename the fields that the field extractor finds¹. This method is simpler and faster than the regular expression method, but it may not work well with complex or irregular data formats¹.

Reference:

1: Build field extractions with the field extractor - Splunk Documentation

NEW QUESTION 83

- (Exam Topic 2)

Which of the following objects can a calculated field use as a source?

- A. An alias of a field.
- B. A field added by an automatic lookup.
- C. The tag field.
- D. The eventtype field.

Answer: B

Explanation:

The correct answer is B. A field added by an automatic lookup.

A calculated field is a field that is added to events at search time by using an eval expression. A calculated field can use the values of two or more fields that are already present in the events to perform calculations. A calculated field can use any field as a source, as long as the field is extracted before the calculated field is defined¹.

An automatic lookup is a way to enrich events with additional fields from an external source, such as a CSV file or a database. An automatic lookup can add fields to events based on the values of existing fields, such as host, source, sourcetype, or any other extracted field². An automatic lookup is performed before the calculated fields are defined, so the fields added by the lookup can be used as sources for the calculated fields³.

Therefore, a calculated field can use a field added by an automatic lookup as a source. References:

- About calculated fields
- About lookups
- Search time processing

NEW QUESTION 85

- (Exam Topic 2)

How many ways are there to access the Field Extractor Utility?

- A. 3
- B. 4
- C. 1
- D. 5

Answer: A

NEW QUESTION 89

- (Exam Topic 2)

When creating a data model, which root dataset requires at least one constraint?

- A. Root transaction dataset
- B. Root event dataset
- C. Root child dataset
- D. Root search dataset

Answer: B

Explanation:

The correct answer is B. Root event dataset. This is because root event datasets are defined by a constraint that filters out events that are not relevant to the dataset. A constraint for a root event dataset is a simple search that returns a fairly wide range of data, such as sourcetype=access_combined. Without a constraint, a root event dataset would include all the events in the index, which is not useful for data modeling. You can learn more about how to design data models and add root event datasets from the Splunk documentation¹. The other options are incorrect because root transaction datasets and root search datasets have different ways of defining their datasets, such as transaction definitions or complex searches, and root child datasets are not a valid type of root dataset.

NEW QUESTION 92

- (Exam Topic 2)

Which of the following statements best describes a macro?

- A. A macro is a method of categorizing events based on a search.
- B. A macro is a way to associate an additional (new) name with an existing field name.
- C. A macro is a portion of a search that can be reused in multiple place
- D. A macro is a knowledge object that enables you to schedule searches for specific events.

Answer: C

Explanation:

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.

References:

- About event types
- About field aliases
- About alerts
- Define search macros in Settings
- Use search macros in searches

NEW QUESTION 94

- (Exam Topic 2)

Which of the following examples would use a POST workflow action?

- A. Perform an external IP lookup based on a domain value found in events.
- B. Use the field values in an HTTP error event to create a new ticket in an external system.
- C. Launch secondary Splunk searches that use one or more field values from selected events.
- D. Open a web browser to look up an HTTP status code.

Answer: B

Explanation:

The correct answer is B. Use the field values in an HTTP error event to create a new ticket in an external system.

A workflow action is a knowledge object that enables a variety of interactions between fields in events and other web resources. Workflow actions can create HTML links, generate HTTP POST requests, or launch secondary searches based on field values¹.

There are three types of workflow actions that can be set up using Splunk Web: GET, POST, and Search².

➤ GET workflow actions create typical HTML links to do things like perform Google searches on specific values or run domain name queries against external WHOIS databases².

➤ POST workflow actions generate an HTTP POST request to a specified URI. This action type enables you to do things like creating entries in external issue management systems using a set of relevant field values².

➤ Search workflow actions launch secondary searches that use specific field values from an event, such as a search that looks for the occurrence of specific combinations of ipaddress and http_status field values in your index over a specific time range².

Therefore, the example that would use a POST workflow action is B. Use the field values in an HTTP error event to create a new ticket in an external system. This example requires sending an HTTP POST request to the URI of the external system with the field values from the event as arguments.

The other examples would use different types of workflow actions. These examples are:

➤ A. Perform an external IP lookup based on a domain value found in events: This example would use a GET workflow action to create a link to an external IP lookup service with the domain value as a parameter.

➤ C. Launch secondary Splunk searches that use one or more field values from selected events: This example would use a Search workflow action to run another Splunk search with the field values from the event as search terms.

➤ D. Open a web browser to look up an HTTP status code: This example would also use a GET workflow action to create a link to a web page that explains the meaning of the HTTP status code.

References:

➤ Splaxon:Workflowaction

➤ About workflow actions in Splunk Web

NEW QUESTION 96

- (Exam Topic 2)

This is what Splunk uses to categorize the data that is being indexed.

- A. Host
- B. Sourcetype
- C. Index
- D. Source

Answer: B

NEW QUESTION 100

- (Exam Topic 2)

Which of the following are valid options to speed up reports? (Select all the apply.)

- A. Edit permissions
- B. Edit description
- C. Edit acceleration
- D. Edit schedule

Answer: C

Explanation:

One of the valid options to speed up reports is to edit acceleration, which means that you can enable summary indexing or data model acceleration for your reports to improve their performance². Summary indexing allows you to create reports that run over large amounts of data by storing the results of scheduled searches in a summary index and using that index for faster reporting². Data model acceleration allows you to create reports that use data models by creating and storing summaries of the data model datasets and using them for faster reporting². Therefore, option C is correct, while options A, B and D are incorrect because they are not options to speed up reports.

NEW QUESTION 105

- (Exam Topic 2)

This function of the stats command allows you to return the sample standard deviation of a field.

- A. stdev
- B. dev
- C. count deviation
- D. by standarddev

Answer: A

NEW QUESTION 106

- (Exam Topic 2)

Tags can reference which of the following knowledge objects?

- A. Lookups and event types only.
- B. Extracted fields, field aliases, calculated fields, lookups, and event types.
- C. Tags cannot reference any of these knowledge objects because tags are the last knowledge objects generated in the search-time operation sequence.
- D. Extracted fields, calculated fields, and field aliases only.

Answer: B

Explanation:

Tags are a type of knowledge object that enable you to assign descriptive keywords to events. Tags can reference any of the following knowledge objects: extracted fields, field aliases, calculated fields, lookups, and event types. Tags cannot reference other tags or search macros. Tags are applied to events at search time based on the values of the fields that they reference2

1: Splunk Core Certified Power User Track, page 10. 2: Splunk Documentation, About tags and aliases.

NEW QUESTION 107

- (Exam Topic 2)

Which command can include both an over and a by clause to divide results into sub-groupings?

- A. chart
- B. stats
- C. xyseries
- D. transaction

Answer: A

NEW QUESTION 109

- (Exam Topic 2)

Which field will be used to populate the field if the productName and product:d fields have values for a given event?

| eval productINFO=coalesce(productName,productid)

- A. Both field values will be used and the product INFO field will become a multivalue field for the given event.
- B. The value for the productName field because it appears first.
- C. Neither field value will be used and the field will be assigned a NULL value for the given event.
- D. The value for the field because it appears second.

Answer: B

Explanation:

The correct answer is B. The value for the productName field because it appears first.

The coalesce function is an eval function that takes an arbitrary number of arguments and returns the first value that is not null. A null value means that the field has no value at all, while an empty value means that the field has a value, but it is "" or zero-length1.

The coalesce function can be used to combine fields that have different names but represent the same data, such as IP address or user name. The coalesce function can also be used to rename fields for clarity or convenience2.

The syntax for the coalesce function is: coalesce(<field1>,<field2>,...)

The coalesce function will return the value of the first field that is not null in the argument list. If all fields are null, the coalesce function will return null.

For example, if you have a set of events where the IP address is extracted to either clientip or ipaddress, you can use the coalesce function to define a new field called ip, that takes the value of either clientip or ipaddress, depending on which is not null:

| eval ip=coalesce(clientip,ipaddress)

In your example, you have a set of events where the product name is extracted to either productName or productid, and you use the coalesce function to define a new field called productINFO, that takes the value of either productName or productid, depending on which is not null:

| eval productINFO=coalesce(productName,productid)

If both productName and productid fields have values for a given event, the coalesce function will return the value of the productName field because it appears first in the argument list. The productid field will be ignored by the coalesce function.

Therefore, the value for the productName field will be used to populate the productINFO field if both fields have values for a given event.

References:

➤ Search Command> Coalesce

➤ USAGE OF SPLUNK EVAL FUNCTION : COALESCE

NEW QUESTION 111

- (Exam Topic 2)

The stats command will create a _____ by default.

- A. Table
- B. Report
- C. Pie chart

Answer: A

NEW QUESTION 114

- (Exam Topic 2)

A user wants to create a new field alias for a field that appears in two sourcetypes. How many field aliases need to be created?

- A. One.
- B. Two.
- C. It depends on whether the original fields have the same name.
- D. It depends on whether the two sourcetypes are associated with the same index.

Answer: B

NEW QUESTION 117

- (Exam Topic 2)

Highlighted search terms indicate _____ search results in Splunk.

- A. Display as selected fields.
- B. Sorted

- C. Charted based on time
- D. Matching

Answer: D

Explanation:

Highlighted search terms indicate matching search results in Splunk, which means that they show which parts of your events match your search string². For example, if you search for error OR fail, Splunk will highlight error or fail in your events to show which events match your search string². Therefore, option D is correct, while options A, B and C are incorrect because they are not indicated by highlighted search terms.

NEW QUESTION 120

- (Exam Topic 2)

Which of these is NOT a field that is automatically created with the transaction command?

- A. maxcount
- B. duration
- C. eventcount

Answer: A

NEW QUESTION 124

- (Exam Topic 2)

Which of the following searches will return events containing a tag named Privileged?

- A. tag=Priv
- B. tag=Priv*
- C. tag=priv*
- D. tag=privileged

Answer: B

Explanation:

The tag=Priv* search will return events containing a tag named Privileged, as well as any other tag that starts with Priv. The asterisk (*) is a wildcard character that matches zero or more characters. The other searches will not match the exact tag name.

NEW QUESTION 126

- (Exam Topic 2)

Calculated fields can be based on which of the following?

- A. Tags
- B. Extracted fields
- C. Output fields for a lookup
- D. Fields generated from a search string

Answer: B

Explanation:

"Calculated fields can reference all types of field extractions and field aliasing, but they cannot reference lookups, event types, or tags."

NEW QUESTION 131

- (Exam Topic 2)

Which search retrieves events with the event type web_errors?

- A. tag=web_errors
- B. eventtype=web_errors
- C. eventtype "web errors"
- D. eventtype (web_errors)

Answer: B

Explanation:

The correct answer is B. eventtype=web_errors.

An event type is a way to categorize 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 reports¹.

To search for events that have a specific event type, you need to use the eventtype field with the name of the event type as the value. The syntax for this is:

eventtype=<event_type_name>

For example, if you want to search for events that have the event type web_errors, you can use the following syntax:

eventtype=web_errors

This will return only the events that match the search criteria defined by the web_errors event type.

The other options are not correct because they use different syntax or fields that are not related to event types. These options are:

- A. tag=web_errors: This option uses the tag field, which is a way to add descriptive keywords to events based on field values. Tags are different from event types, although they can be used together. Tags can be used to filter and group events by common characteristics².
- C. eventtype "web errors": This option uses quotation marks around the event type name, which is not valid syntax for the eventtype field. Quotation marks are used to enclose phrases or exact matches in a search³.
- D. eventtype (web_errors): This option uses parentheses around the event type name, which is also not valid syntax for the eventtype field. Parentheses are used to group expressions or terms in a search³.

References:

- About event types
- About tags
- Search command cheatsheet

NEW QUESTION 135

- (Exam Topic 2)

_____ datasets can be added to root dataset to narrow down the search

- A. parent
- B. extracted
- C. event
- D. child

Answer: D

Explanation:

Child datasets can be added to root datasets to narrow down the search. Datasets are collections of events that represent your data in a structured and hierarchical way. Datasets can be created by using commands such as datamodel or pivot. Datasets can have different types, such as events, search, transaction, etc. Datasets can also have different levels, such as root or child. Root datasets are base datasets that contain all events from a data model or an index. Child datasets are derived datasets that contain a subset of events from a parent dataset based on some constraints, such as search terms, fields, time range, etc. Child datasets can be added to root datasets to narrow down the search and filter out irrelevant events.

NEW QUESTION 140

- (Exam Topic 2)

A macro has another macro nested within it, and this inner macro requires an argument. How can the user pass this argument into the SPL?

- A. An argument can be passed through the outer macro.
- B. An argument can be passed to the outer macro by nesting parentheses.
- C. There is no way to pass an argument to the inner macro.
- D. An argument can be passed to the inner macro by nesting parentheses.

Answer: D

Explanation:

The correct answer is D. An argument can be passed to the inner macro by nesting parentheses.

A search macro is a way to reuse a piece of SPL code in different searches. A search macro can take arguments, which are variables that can be replaced by different values when the macro is called. A search macro can also contain another search macro within it, which is called a nested macro. A nested macro can also take arguments, which can be passed from the outer macro or directly from the search string.

To pass an argument to the inner macro, you need to use parentheses to enclose the argument value and separate it from the outer macro argument. For example, if you have a search macro named outer_macro (1) that contains another search macro named inner_macro (2), and both macros take one argument each, you can pass an argument to the inner macro by using the following syntax:

```
outer_macro (argument1, inner_macro (argument2))
```

This will replace the argument1 and argument2 with the values you provide in the search string. For example, if you want to pass “foo” as the argument1 and “bar” as the argument2, you can write:

```
outer_macro ("foo", inner_macro ("bar"))
```

This will expand the macros with the corresponding arguments and run the SPL code contained in them. References:

- Search macro examples
- Use search macros in searches

NEW QUESTION 141

- (Exam Topic 2)

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

- A. maxpause
- B. endswith
- C. maxduration
- D. maxspan

Answer: D

Explanation:

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.

NEW QUESTION 146

- (Exam Topic 2)

Which of the following expressions could be used to create a calculated field called gigabytes?

- A. eval sc_bytes(1024/1024)
- B. | eval negabytes=sc_bytes(1024/1024)
- C. megabytes=sc_bytes(1024/1024)
- D. sc_bytas(1024/1024)

Answer: B

NEW QUESTION 148

- (Exam Topic 2)

Clicking a SEGMENT on a chart, _____.

- A. drills down for that value
- B. highlights the field value across the chart
- C. adds the highlighted value to the search criteria

Answer: C

NEW QUESTION 151

- (Exam Topic 2)

which of the following are valid options with the chart command

- A. useother
- B. usenull
- C. fillfield
- D. usefiled

Answer: AB

NEW QUESTION 156

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SPLK-1002 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SPLK-1002-dumps.html>