

Splunk

Exam Questions SPLK-1002

Splunk Core Certified Power User Exam



NEW QUESTION 1

- (Exam Topic 1)

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?

- A. | datamodel web search | filed web *
- B. | Search datamodel web web | filed web*
- C. | datamodel web web field | search web*
- D. Datamodel=web | search web | filed web*

Answer: A

Explanation:

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.

NEW QUESTION 2

- (Exam Topic 1)

When multiple event types with different color values are assigned to the same event, what determines the color displayed for the events?

- A. Rank
- B. Weight
- C. Priority
- D. Precedence

Answer: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/SplunkCloud/8.0.2003/Knowledge/Defineeventtypes> When multiple event types with different color values are assigned to the same event, the color displayed for the events is determined by the priority of the event types. The priority is a numerical value that indicates how important an event type is. The higher the priority, the more important the event type. The event type with the highest priority will determine the color of the event.

NEW QUESTION 3

- (Exam Topic 1)

Which of the following statements describes field aliases?

- A. Field alias names replace the original field name.
- B. Field aliases can be used in lookup file definitions.
- C. Field aliases only normalize data across sources and sourcetypes.
- D. Field alias names are not case sensitive when used as part of a search.

Answer: B

Explanation:

Field aliases are alternative names for fields in Splunk. Field aliases can be used to normalize data across different sources and sourcetypes that have different field names for the same concept. For example, you can create a field alias for src_ip that maps to clientip, source_address, or any other field name that represents the source IP address in different sourcetypes. Field aliases can also be used in lookup file definitions to map fields in your data to fields in the lookup file. For example, you can use a field alias for src_ip to map it to ip_address in a lookup file that contains geolocation information for IP addresses. Field alias names do not replace the original field name, but rather create a copy of the field with a different name. Field alias names are case sensitive when used as part of a search, meaning that src_ip and SRC_IP are different fields.

NEW QUESTION 4

- (Exam Topic 1)

What does the fillnull command replace null values with, if the value argument is not specified?

- A. N/A
- B. NaN
- C. NULL

Answer: A

Explanation:

Reference: <https://answers.splunk.com/answers/653427/fillnull-doesnt-work-without-specifying-a-field.html> The fillnull command is a search command that replaces null values with a specified value or 0 if no value is specified. Null values are values that are missing, empty, or undefined in Splunk. The fillnull command can replace null values for all fields or for specific fields. The fillnull command can take an optional argument called value that specifies the value to replace null values with. If no value argument is specified, the fillnull command will replace null values with 0 by default.

NEW QUESTION 5

- (Exam Topic 1)

Which of the following actions can the eval command perform?

- A. Remove fields from results.
- B. Create or replace an existing field.
- C. Group transactions by one or more fields.
- D. Save SPL commands to be reused in other searches.

Answer: B

Explanation:

The eval command is used to create new fields or modify existing fields based on an expression². The eval command can perform various actions such as calculations, conversions, string manipulations and more². One of the actions that the eval command can perform is to create or replace an existing field with a new value based on an expression². For example, `| eval status=if(status="200","OK","ERROR")` will create or replace status field with either OK or ERROR depending on the original value of status². Therefore, option B is correct, while options A, C and D are incorrect because they are not actions that the eval command can perform.

NEW QUESTION 6

- (Exam Topic 1)

Which of the following statements is true, especially in large environments?

- A. Use the stats command when you next to group events by two or more fields.
- B. The stats command is faster and more efficient than the transaction command
- C. The transaction command is faster and more efficient than the stats command.
- D. Use the transaction command when you want to see the results of a calculation.

Answer: B

Explanation:

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

The stats command is faster and more efficient than the transaction command, especially in large environments. The stats command is used to calculate summary statistics on the events, such as count, sum, average, etc. The stats command can group events by one or more fields or by time buckets. The stats command does not create new events from groups of events, but rather creates new fields with statistical values. The transaction command is used to group events into transactions based on some common characteristics, such as fields, time, or both. The transaction command creates new events from groups of events that share one or more fields. The transaction command also creates some additional fields for each transaction, such as duration, eventcount, starttime, etc. The transaction command is slower and more resource-intensive than the stats command because it has to process more data and create more events and fields.

NEW QUESTION 7

- (Exam Topic 1)

What do events in a transaction have in common?

- A. All events in a transaction must have the same timestamp.
- B. All events in a transaction must have the same sourcetype.
- C. All events in a transaction must have the exact same set of fields.
- D. All events in a transaction must be related by one or more fields.

Answer: D

Explanation:

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

A transaction is a group of events that share some common characteristics, such as fields, time, or both. A transaction can be created by using the transaction command or by defining an event type with `transactiontype=true` in props.conf. Events in a transaction have one or more fields in common that relate them to each other. For example, you can create a transaction based on JSESSIONID, which is a unique identifier for each user session in web logs. Events in a transaction do not have to have the same timestamp, sourcetype, or exact same set of fields. They only have to share one or more fields that define the transaction.

NEW QUESTION 8

- (Exam Topic 1)

After manually editing a regular expression (regex), which of the following statements is true?

- A. Changes made manually can be reverted in the Field Extractor (FX) UI.
- B. It is no longer possible to edit the field extraction in the Field Extractor (FX) UI.
- C. It is not possible to manually edit a regular expression (regex) that was created using the Field Extractor (FX) UI.
- D. The Field Extractor (FX) UI keeps its own version of the field extraction in addition to the one that was manually edited.

Answer: B

Explanation:

After manually editing a regular expression (regex) that was created using the Field Extractor (FX) UI, it is no longer possible to edit the field extraction in the FX UI. The FX UI is a tool that helps you extract fields from your data using delimiters or regular expressions. The FX UI can generate a regex for you based on your selection of sample values or you can enter your own regex in the FX UI. However, if you edit the regex manually in the props.conf file, the FX UI will not be able to recognize the changes and will not let you edit the field extraction in the FX UI anymore. You will have to use the props.conf file to make any further changes to the field extraction. Changes made manually cannot be reverted in the FX UI, as the FX UI does not keep track of the changes made in the props.conf file. It is possible to manually edit a regex that was created using the FX UI, as long as you do it in the props.conf file. Therefore, only statement B is true about manually editing a regex.

NEW QUESTION 9

- (Exam Topic 1)

Which of the following statements describe GET workflow actions?

- A. GET workflow actions must be configured with POST arguments.
- B. Configuration of GET workflow actions includes choosing a sourcetype.
- C. Label names for GET workflow actions must include a field name surrounded by dollar signs.
- D. GET workflow actions can be configured to open the URT link in the current window or in a new window

Answer: D

Explanation:

GET workflow actions are custom actions that open a URL link when you click on a field value in your search results. GET workflow actions can be configured with various options, such as label name, base URL, URI parameters, app context, etc. One of the options is to choose whether to open the URL link in the current window or in a new window. GET workflow actions do not have to be configured with POST arguments, as they use GET method to send requests to web servers. Configuration of GET workflow actions does not include choosing a sourcetype, as they do not generate any data in Splunk. Label names for GET workflow actions must include a field name surrounded by dollar signs, as this indicates the field value that will be used to replace the variable in the URL link.

NEW QUESTION 10

- (Exam Topic 1)

Which of the following statements describes POST workflow actions?

- A. POST workflow actions are always encrypted.
- B. POST workflow actions cannot use field values in their URI.
- C. POST workflow actions cannot be created on custom sourcetypes.
- D. POST workflow actions can open a web page in either the same window or a new .

Answer: D

Explanation:

A workflow action is a link that appears when you click an event field value in your search results¹. A workflow action can open a web page or run another search based on the field value¹. There are two types of workflow actions: GET and POST¹. A GET workflow action appends the field value to the end of a URI and opens it in a web browser¹. A POST workflow action sends the field value as part of an HTTP request to a web server¹. You can configure a workflow action to open a web page in either the same window or a new window¹. Therefore, option D is correct, while options A, B and C are incorrect.

NEW QUESTION 10

- (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 15

- (Exam Topic 1)

Which of the following statements describes the command below (select all that apply) Sourcetype=access_combined | transaction JSESSIONID

- A. An additional field named maxspan is created.
- B. An additional field named duration is created.
- C. An additional field named eventcount is created.
- D. Events with the same JSESSIONID will be grouped together into a single event.

Answer: BCD

Explanation:

The command sourcetype=access_combined | transaction JSESSIONID does three things:

- It filters the events by the sourcetype access_combined, which is a predefined sourcetype for Apache web server logs.
 - It groups the events by the field JSESSIONID, which is a unique identifier for each user session.
 - It creates a single event from each group of events that share the same JSESSIONID value. This single event will have some additional fields created by the transaction command, such as duration, eventcount, and starttime.
- Therefore, the statements B, C, and D are true.

NEW QUESTION 16

- (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 20

- (Exam Topic 1)

When using the Field Extractor (FX), which of the following delimiters will work? (select all that apply)

- A. Tabs
- B. Pipes
- C. Colons
- D. Spaces

Answer: ABD

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/FXSelectMethodstep> <https://community.splunk.com/t5/Splunk-Search/Field-Extraction-Separate-on-Colon/m-p/29751>

The Field Extractor (FX) is a tool that helps you extract fields from your data using delimiters or regular expressions. Delimiters are characters or strings that separate fields in your data. Some of the delimiters that will work with FX are:

Tabs: horizontal spaces that align text in columns.

Pipes: vertical bars that often indicate logical OR operations. Spaces: blank characters that separate words or symbols. Therefore, the delimiters A, B, and D will work with FX.

NEW QUESTION 23

- (Exam Topic 1)

Which of the following are required to create a POST workflow action?

- A. Label, URI, search string.
- B. XMI attributes, URI, name.
- C. Label, URI, post arguments.
- D. URI, search string, time range picker.

Answer: C

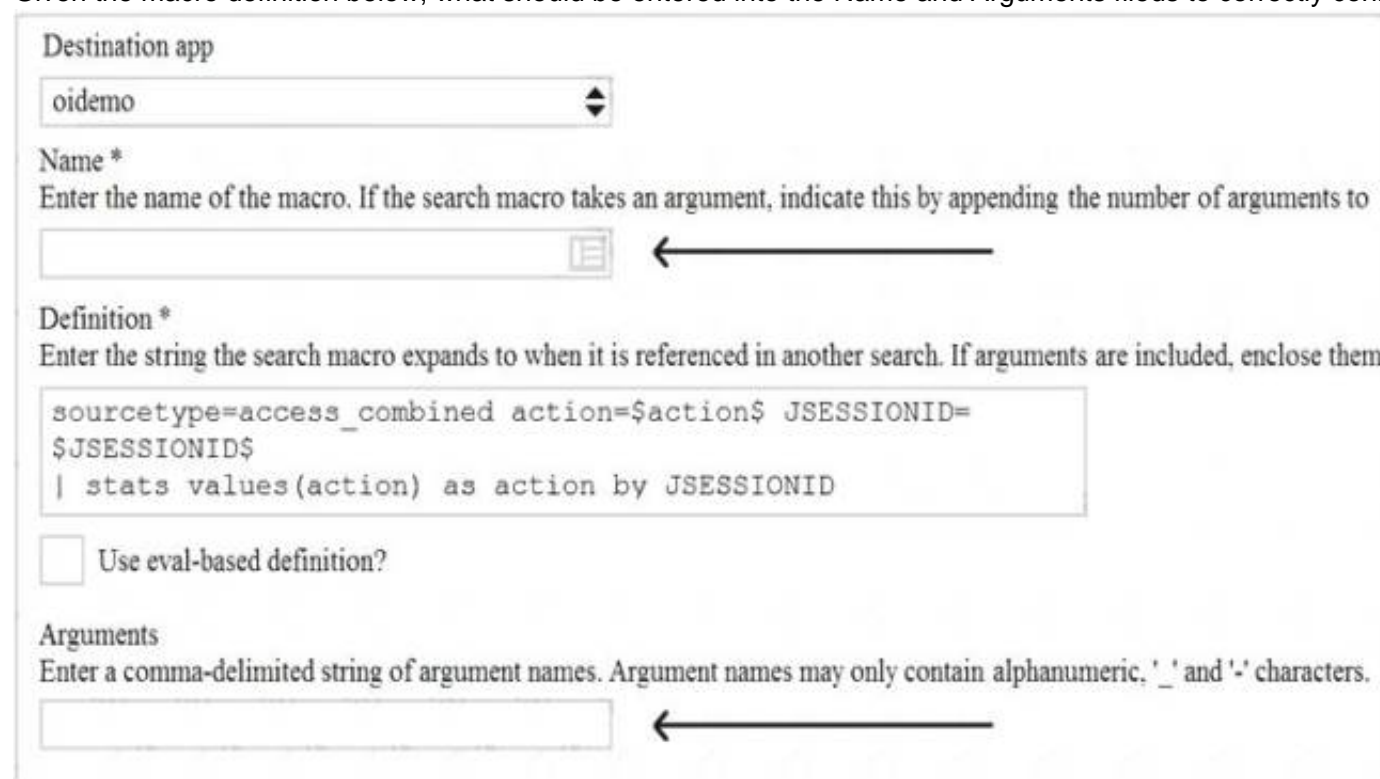
Explanation:

POST workflow actions are custom actions that send a POST request to a web server when you click on a field value in your search results. POST workflow actions can be configured with various options, such as label name, base URL, URI parameters, post arguments, app context, etc. One of the options that are required to create a POST workflow action is post arguments. Post arguments are key-value pairs that are sent in the body of the POST request to provide additional information to the web server. Post arguments can include field values from your data by using dollar signs around the field names.

NEW QUESTION 24

- (Exam Topic 1)

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



- 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 27

- (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 32

- (Exam Topic 1)

A calculated field maybe based on which of the following?

- A. Lookup tables
- B. Extracted fields
- C. Regular expressions
- D. Fields generated within a search string

Answer: B

Explanation:

As mentioned before, a calculated field is a field that you create based on the value of another field or fields². A calculated field 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 pairs². Therefore, option B is correct, while options A, C and D are incorrect because they are not types of fields that a calculated field can be based on.

NEW QUESTION 35

- (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 36

- (Exam Topic 1)

When using timechart, how many fields can be listed after a by clause?

- A. because timechart doesn't support using a by clause.
- B. because _time is already implied as the x-axis.
- C. because one field would represent the x-axis and the other would represent the y-axis.
- D. There is no limit specific to timechart.

Answer: B

Explanation:

The timechart command is used to create a time-series chart of statistical values based on your search results². You can use the timechart command with a by clause to split the results by one or more fields and create multiple series in the chart². However, you can only list one field after the by clause when using the timechart command because _time is already implied as the x-axis of the chart². Therefore, option B is correct, while options A, C and D are incorrect.

NEW QUESTION 41

- (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 42

- (Exam Topic 1)

Which of the following statements describe data model acceleration? (select all that apply)

- A. Root events cannot be accelerated.
- B. Accelerated data models cannot be edited.
- C. Private data models cannot be accelerated.
- D. You must have administrative permissions or the `accelerate_dacamodel` capability to accelerate a data model.

Answer: BCD

Explanation:

Data model acceleration is a feature that speeds up searches on data models by creating and storing summaries of the data model datasets¹. To enable data model acceleration, you must have administrative permissions or the `accelerate_datamodel` capability¹. Therefore, option D is correct. Accelerated data models cannot be edited unless you disable the acceleration first¹. Therefore, option B is correct. Private data models cannot be accelerated because they are not visible to other users¹. Therefore, option C is correct. Root events can be accelerated as long as they are not based on a search string¹. Therefore, option A is incorrect.

NEW QUESTION 44

- (Exam Topic 1)

To identify all of the contributing events within a transaction that contains at least one REJECT event, which syntax is correct?

- A. `Index-main | REJECT trans sessionid`
- B. `Index-main | transaction sessionid | search REJECT`
- C. `Index=main | transaction sessionid | whose transaction=reject`
- D. `Index=main | transaction sessionid | where transaction=reject`

Answer: B

Explanation:

The transaction command is used to group events that share a common value for one or more fields into transactions². The transaction command assigns a transaction ID to each group of events and creates new fields such as `duration`, `eventcount` and `eventlist` for each transaction². To identify all of the contributing events within a transaction that contains at least one REJECT event, you can use the following syntax: `index=main | transaction sessionid | search REJECT`². This search will first group the events by `sessionid`, then filter out the transactions that do not contain REJECT in any of their events². Therefore, option B is correct, while options A, C and D are incorrect because they do not follow the correct syntax for using the transaction command or the search command.

NEW QUESTION 46

- (Exam Topic 1)

What does the transaction command do?

- A. Groups a set of transactions based on time.
- B. Creates a single event from a group of events.
- C. Separates two events based on one or more values.
- D. Returns the number of credit card transactions found in the event logs.

Answer: B

Explanation:

The transaction command is a search command that creates a single event from a group of events that share some common characteristics. The transaction command can group events based on fields, time, or both. The transaction command can also create some additional fields for each transaction, such as `duration`, `eventcount`, `starttime`, etc. The transaction command does not group a set of transactions based time, but rather groups a set of events into a transaction based on time. The transaction command does not separate two events based on one or more values, but rather joins multiple events based on one or more values. The transaction command does not return the number of credit card transactions found in the event logs, but rather creates transactions from the events that match the search criteria.

NEW QUESTION 47

- (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 48

- (Exam Topic 1)

Data model fields can be added using the Auto-Extracted method. Which of the following statements describe Auto-Extracted fields? (select all that apply)

- A. Auto-Extracted fields can be hidden in Pivot.
- B. Auto-Extracted fields can have their data type changed.
- C. Auto-Extracted fields can be given a friendly name for use in Pivot.
- D. Auto-Extracted fields can be added if they already exist in the dataset with constraints.

Answer: ABCD

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.

NEW QUESTION 50

- (Exam Topic 1)

Which of the following workflow actions can be executed from search results? (select all that apply)

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

Answer: ABD

Explanation:

As mentioned before, there are two types of workflow actions: GET and POST1. Both types of workflow actions can be executed from search results by clicking on an event field value that has a workflow action configured for it1. Another type of workflow action is Search, which runs another search based on the field value1. Therefore, options A, B and D are correct, while option C is incorrect because LOOKUP is not a type of workflow action.

NEW QUESTION 52

- (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 57

- (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 60

- (Exam Topic 1)

When creating a Search workflow action, which field is required?

- A. Search string
- B. Data model name
- C. Permission setting
- D. An eval statement

Answer: A

Explanation:

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.

NEW QUESTION 65

- (Exam Topic 1)

A user wants to convert numeric field values to strings and also to sort on those values. Which command should be used first, the eval or the sort?

- A. It doesn't matter whether eval or sort is used first.
- B. Convert the numeric to a string with eval first, then sort.
- C. Use sort first, then convert the numeric to a string with eval.
- D. You cannot use the sort command and the eval command on the same field.

Answer: C

Explanation:

The eval command is used to create new fields or modify existing fields based on an expression². The sort command is used to sort the results by one or more fields in ascending or descending order². If you want to convert numeric field values to strings and also sort on those values, you should use the sort command first, then use the eval command to convert the values to strings². This way, the sort command will use the original numeric values for sorting, rather than the converted string values which may not sort correctly. Therefore, option C is correct, while options A, B and D are incorrect.

NEW QUESTION 66

- (Exam Topic 1)

Which of the following statements describe the search string below?

| datamodel Application_State All_Application_State search

- A. Evenrches would return a report of sales by state.
- B. Events will be returned from the data model named Application_State.
- C. Events will be returned from the data model named All_Application_state.
- D. No events will be returned because the pipe should occur after the datamodel command

Answer: B

Explanation:

The search string below returns events from the data model named Application_State.

| datamodel Application_State All_Application_State search The search string does the following:

- It uses the datamodel command to access a data model in Splunk. The datamodel command takes two arguments: the name of the data model and the name of the dataset within the data model.
- It specifies the name of the data model as Application_State. This is a predefined data model in Splunk that contains information about web applications.
- It specifies the name of the dataset as All_Application_State. This is a root dataset in the data model that contains all events from all child datasets.
- It uses the search command to filter and transform the events from the dataset. The search command can use any search criteria or command to modify the results.

Therefore, the search string returns events from the data model named Application_State.

NEW QUESTION 69

- (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 73

- (Exam Topic 2)

This function of the stats command allows you to return the middle-most value of field X.

- A. Median(X)
- B. Eval by X
- C. Fields(X)
- D. Values(X)

Answer: A

NEW QUESTION 78

- (Exam Topic 2)

When using a field value variable with a Workflow Action, which punctuation mark will escape the data

- A. *
- B. !
- C. ^
- D. #

Answer: B

Explanation:

When using a field value variable with a Workflow Action, the exclamation mark (!) will escape the data. A Workflow Action is a custom action that performs a task when you click on a field value in your search results. A Workflow Action can be configured with various options, such as label name, base URL, URI parameters, post arguments, app context, etc. A field value variable is a placeholder for the field value that will be used to replace the variable in the URL or post argument of the Workflow Action. A field value variable is written as fieldname, where field_name is the name of the field whose value will be used. However, if the field value contains special characters that need to be escaped, such as spaces, commas, etc., you can use the exclamation mark (!) before and after the field value variable to escape the data. For example, if you have a field value variable host, you can write it as !\$host! to escape any special characters in the host field value. Therefore, option B is the correct answer.

NEW QUESTION 81

- (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 83

- (Exam Topic 2)

In this search, _____ will appear on the y-axis. SEARCH: sourcetype=access_combined status!=200 | chart count over host

- A. status
- B. host
- C. count

Answer: C

Explanation:

In this search, count will appear on the y-axis². This search uses the chart command to create a chart of the count of events over host for events that have status not equal to 200². The chart command creates a table with one column for each value of the field after the over clause and one row for each value of the field after the by clause (if any)². The values in the table are calculated by applying the function before the over clause to the events in each group². In this case, the chart command creates a table with one column for each host and one row for the count of events for each host. The y-axis of the chart shows the values of the count function applied to each host. Therefore, option C is correct, while options A and B are incorrect because they appear on the x-axis or as labels of the chart.

NEW QUESTION 88

- (Exam Topic 2)

What type of command is eval?

- A. Streaming in some modes
- B. Report generating
- C. Distributable streaming
- D. Centralized streaming

Answer: C

Explanation:

The correct answer is C. Distributable streaming. This is because the eval command is a type of command that can run on the indexers before the results are sent to the search head. This reduces the amount of data that needs to be transferred and improves the search performance. Distributable streaming commands can operate on each event or result individually, without depending on other events or results. You can learn more about the types of commands and how they affect search performance from the Splunk documentation¹.

NEW QUESTION 91

- (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 93

- (Exam Topic 2)

Field aliases are used to _____ data

- A. clean
- B. transform
- C. calculate
- D. normalize

Answer: D

NEW QUESTION 98

- (Exam Topic 2)

Which of the following search control will not re-rerun the search? (Select all that apply.)

- A. zoom out
- B. selecting a bar on the timeline
- C. deselect
- D. selecting a range of bars on the timelines

Answer: BCD

Explanation:

The timeline is a graphical representation of your search results that shows the distribution of events over time². You can use the timeline to zoom in or out of a specific time range or to select one or more bars on the timeline to filter your results by that time range². However, these actions will not re-run the search, but rather refine the existing results based on the selected time range². Therefore, options B, C and D are correct, while option A is incorrect because zooming out will re-run the search with a broader time range.

NEW QUESTION 99

- (Exam Topic 2)

What is the correct syntax to find events associated with a tag?

- A. tag:<field>=<value>
- B. tags=<value>
- C. tags:<field>=<value>
- D. tag=<value>

Answer: D

Explanation:

The correct syntax to find events associated with a tag in Splunk is `tag=<value>1`. So, the correct answer is D. `tag=<value>`. This syntax allows you to annotate specified fields in your search results with tags¹.

In Splunk, tags are a type of knowledge object that you can use to add meaningful aliases to field values in your data¹. For example, if you have a field called `status_code` in your data, you might have different status codes like 200, 404, 500, etc. You can create tags for these status codes like `success` for 200, `not_found` for 404, and `server_error` for 500. Then, you can use the `tag` command in your searches to find events associated with these tags¹.

Here is an example of how you can use the `tag` command in a search: `index=main sourcetype=access_combined | tag status_code`

In this search, the `tag` command annotates the `status_code` field in the search results with the corresponding tags. If you have tagged the status code 200 with `success`, the status code 404 with `not_found`, and the status code 500 with `server_error`, the search results will include these tags¹.

You can also use the `tag` command with a specific tag value to find events associated with that tag. For example, the following search finds all events where the status code is tagged with `success`:

`index=main sourcetype=access_combined | tag status_code | search tag::status_code=success`

In this search, the `tag` command annotates the `status_code` field with the corresponding tags, and the `search` command filters the results to include only events where the `status_code` field is tagged with `success`¹.

NEW QUESTION 104

- (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 108

- (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 111

- (Exam Topic 2)

The `transaction` command allows you to _____ events across multiple sources

- A. duplicate
- B. correlate
- C. persist
- D. tag

Answer: B

Explanation:

The `transaction` command allows you to correlate events across multiple sources. The `transaction` command is a search command that allows you to group events into transactions based on some common characteristics, such as fields, time, or both. A transaction is a group of events that share one or more fields that relate them to each other. A transaction can span across multiple sources or sourcetypes that have different formats or structures of data. The `transaction` command can help you correlate events across multiple sources by using the common fields as the basis for grouping. The `transaction` command can also create some additional fields for each transaction, such as `duration`, `eventcount`, `starttime`, etc.

NEW QUESTION 114

- (Exam Topic 2)

What information must be included when using the `datamodel` command?

- A. status field

- B. Multiple indexes
- C. Data model field name.
- D. Data model dataset name.

Answer: D

NEW QUESTION 116

- (Exam Topic 2)

Which of the following statements describes POST workflow actions?

- A. Configuration of a POST workflow action includes choosing a sourcetype.
- B. POST workflow actions can be configured to send email to the URI location.
- C. By default, POST workflow action are shown in both the event and field menus.
- D. POST workflow actions can be configured to send POST arguments to the URI location.

Answer: D

Explanation:

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

NEW QUESTION 120

- (Exam Topic 2)

A user runs the following search:

index—X sourcetype=Y | chart count (domain) as count, sum (price) as sum by product, action usenull=f useother—f

Which of the following table headers match the order this command creates?

- A. The chart command does not allow for multiple statistical functions.
- B. Product, sum: addtocart, sum: remove, sum: purchase, count: addtocart, count: remove, count: purchase
- C. Product, count: addtocart, count: remove, count: purchase, sum: addtocart, sum: remove, sum: purchase
- D. Count: product, sum: product, count: action, sum: action

Answer: C

Explanation:

The correct answer is C. Product, count: addtocart, count: remove, count: purchase, sum: addtocart, sum: remove, sum: purchase1.

In Splunk, the chart command is used to create a table or a chart visualization from your data2. The chart command takes at least one function and one field, and optionally another field to group by2.

In the given search, the chart command is used with two functions (count and sum), two fields (domain and price), and two fields to group by (product and action).

The usenull=f and useother=f options are used to exclude null values and other values from the chart2.

The chart command creates a table with headers that match the order of the fields and functions in the command1. The headers for the count function are prefixed with count:, and the headers for the sum function are prefixed with sum:1. The values of the product and action fields are used as the suffixes for the headers1.

Therefore, the table headers created by this command are Product, count: addtocart, count: remove, count: purchase, sum: addtocart, sum: remove, and sum: purchase1.

NEW QUESTION 125

- (Exam Topic 2)

Data models are composed of one or more of which of the following datasets? (select all that apply)

- A. Transaction datasets
- B. Events datasets
- C. Search datasets
- D. Any child of event, transaction, and search datasets

Answer: ABC

Explanation:

Data model datasets have a hierarchical relationship with each other, meaning they have parent-child relationships. Data models can contain multiple dataset hierarchies. There are three types of dataset hierarchies: event, search, and transaction.

<https://docs.splunk.com/Splexicon:Datamodeldataset>

NEW QUESTION 130

- (Exam Topic 2)

When using the transaction command, what does the argument maxspan do?

- A. Sets the maximum total time between events in a transaction.
- B. Sets the maximum length of all events within a transaction.
- C. Sets the maximum total time between the earliest and latest events in a transaction.
- D. Sets the maximum length that any single event can reach to be included in the transaction.

Answer: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchReference/Transaction>

NEW QUESTION 134

- (Exam Topic 2)

What commands can be used to group events from one or more data sources?

- A. eval, coalesce
- B. transaction, stats
- C. stats, format
- D. top, rare

Answer: B

Explanation:

The transaction and stats commands are two ways to group events from one or more data sources based on common fields or time ranges. The transaction command creates a single event out of a group of related events, while the stats command calculates summary statistics over a group of events. The eval and coalesce commands are used to create or combine fields, not to group events. The format command is used to format the results of a subsearch, not to group events. The top and rare commands are used to rank the most or least common values of a field, not to group events²³

1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, transaction command. 3: Splunk Documentation, stats command.

NEW QUESTION 137

- (Exam Topic 2)

When you mouse over and click to add a search term this (thesE. Boolean operator(s) is(arE. not implied. (Select all that apply).

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

Answer: ABD

Explanation:

When you mouse over and click to add a search term from the Fields sidebar or from an event in your search results, Splunk automatically adds the term to your search string with an implied AND operator². However, this does not apply to some Boolean operators such as OR, NOT and parentheses (). These operators are not implied when you add a search term and you have to type them manually if you want to use them in your search string². Therefore, options A, B and D are correct, while option C is incorrect because AND is implied when you add a search term.

NEW QUESTION 141

- (Exam Topic 2)

What is the Splunk Common Information Model (CIM)?

- A. The CIM is a prerequisite that any data source must meet to be successfully onboarded into Splunk.
- B. The CIM provides a methodology to normalize data from different sources and source types.
- C. The CIM defines an ecosystem of apps that can be fully supported by Splunk.
- D. The CIM is a data exchange initiative between software vendors.

Answer: B

Explanation:

The Splunk Common Information Model (CIM) provides a methodology to normalize data from different sources and source types. The CIM defines a common set of fields and tags for different types of data, such as web, network, email, etc. This allows you to search and analyze data from different sources in a consistent way.

NEW QUESTION 146

- (Exam Topic 2)

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

- A. | chart count by vendor_action, user
- B. | chart count over vendor_action, user
- C. | chart count by vendor_action over user
- D. | chart count over user by vendor_action

Answer: A

Explanation:

<https://docs.splunk.com/Documentation/Splunk/8.1.2/SearchReference/Chart>

NEW QUESTION 147

- (Exam Topic 2)

Consider the the following search run over a time range of last 7 days: index=web sourcetype=access_combined | timechart avg(bytes) by product_nane
Which option is used to change the default time span so that results are grouped into 12 hour intervals?

- A. span=12h
- B. timespan=12h
- C. span=12
- D. timespan=12

Answer: A

Explanation:

The span option is used to specify the time span for the timechart command. The span value can be a number followed by a time unit, such as h for hour, d for day, w for week, etc. The span value determines how the data is grouped into time buckets. For example, span=12h means that the data is grouped into 12-hour intervals. The timespan option is not a valid option for the timechart command²

1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, timechart command.

NEW QUESTION 151

- (Exam Topic 2)

Which of the following commands support the same set of functions?

- A. stats, eval, table
- B. search, where, eval
- C. stats, chart, timechart
- D. transaction, chart, timechart

Answer: C

NEW QUESTION 153

- (Exam Topic 2)

Which statement is true?

- A. Pivot is used for creating datasets.
- B. Data model are randomly structured datasets.
- C. Pivot is used for creating reports and dashboards.
- D. In most cases, each Splunk user will create their own data model.

Answer: C

Explanation:

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

Pivot is used for creating reports and dashboards. Pivot is a tool that allows you to create reports and dashboards from your data models without writing any SPL commands. Pivot can help you visualize and analyze your data using various options, such as filters, rows, columns, cells, charts, tables, maps, etc. Pivot can also help you accelerate your reports and dashboards by using summary data from your accelerated data models.

Pivot is not used for creating datasets or data models. Datasets are collections of events that represent your data in a structured and hierarchical way. Data models are predefined datasets for various domains, such as network traffic, web activity, authentication, etc. Datasets and data models can be created by using commands such as datamodel or pivot.

NEW QUESTION 155

- (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 159

- (Exam Topic 2)

Which of the following eval commands will provide a new value for host from src if it exists?

- A. | eval host = if (isnu11 (src), src, host)
- B. | eval host = if (NOT src = host, src, host)

- C. | eval host = if (src = host, src, host)
D. | eval host = if (isnotnull (src), src, host)

Answer: D

Explanation:

- The eval command is a Splunk command that allows you to create or modify fields using expressions .
- The if function is an expression that evaluates a condition and returns a value based on whether the condition is true or false. The syntax of the if function is if(X,Y,Z), where X is the condition, Y is th value to return if X is true, and Z is the value to return if X is false.
- The isnotnull function is an expression that returns true if the argument is not null, and false otherwise The syntax of the isnotnull function is isnotnull(X), where X is the argument to check.
- Therefore, the expression if (isnotnull (src), src, host) returns the value of src if it is not null, and th value of host otherwise. This means that it will provide a new value for host from src if it exist keep the original value of host otherwise.

NEW QUESTION 160

- (Exam Topic 2)

Which of these search strings is NOT valid:

- A. index=web status=50* | chart count over host, status
B. index=web status=50* | chart count over host by status
C. index=web status=50* | chart count by host, status

Answer: A

Explanation:

This search string is not valid: index=web status=50* | chart count over host,status2. This search string uses an invalid syntax for the chart command. The chart command requires one field after the over clause and optionally one field after the by clause. However, this search string has two fields after the over clause separated by a comma. This will cause a syntax error and prevent the search from running. Therefore, option A is correct, while options B and C are incorrect because they are valid search strings that use the chart command correctly.

NEW QUESTION 163

- (Exam Topic 2)

For the following search, which field populates the x-axis? index=security sourcetype=linux secure | timechart count by action

- A. action
B. source type
C. _time
D. time

Answer: C

Explanation:

The correct answer is C. _time.

The timechart command creates a time series chart with corresponding table of statistics, 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. In this case, the split-by field is action, which means that the chart will have different lines for different actions, such as accept, reject, or fail². The count function will calculate the number of events for each action in each time bin¹.

For example, the following image shows a timechart of the count by action for a similar search³:

As you can see, the x-axis is populated by the _time field, which represents the time range of the search. The y-axis is populated by the count function, which represents the number of events for each action. The legend shows the different values of the action field, which are used to split the chart into different series.

Reference:

2: Timechart Command In Splunk With Example - Mindmajix 1: timechart - Splunk Documentation 3: timechart command examples - Splunk Documentation

NEW QUESTION 168

- (Exam Topic 2)

Which of the following statements describes the use of the Filed Extractor (FX)?

- A. The Field Extractor automatically extracts all field at search time.
B. The Field Extractor uses PERL to extract field from the raw events.
C. Field extracted using the Extracted persist as knowledge objects.
D. Fields extracted using the Field Extractor do not persist and must be defined for each search.

Answer: C

Explanation:

The Field Extractor (FX) is a tool that helps you extract fields from your events using a graphical interface or by manually editing the regular expression². The FX allows you to create field extractions that persist as knowledge objects, which are entities that you create to add knowledge to your data and make it easier to search and analyze². Field extractions are methods that extract fields from your raw data using various techniques such as regular expressions, delimiters or key-value pairs². When you create a field extraction using the FX, you can save it as a knowledge object that applies to your data at search time². You can also manage and share your field extractions with other users in your organization². Therefore, option C is correct, while options A, B and D are incorrect because they do not describe the use of the FX.

NEW QUESTION 173

- (Exam Topic 2)

Which of the following statements describes the use of the Field Extractor (FX)?

- A. The Field Extractor automatically extracts all fields at search time.

- B. The Field Extractor uses PERL to extract fields from the raw events.
- C. Fields extracted using the Field Extractor persist as knowledge objects.
- D. Fields extracted using the Field Extractor do not persist and must be defined for each search.

Answer: C

Explanation:

The statement that fields extracted using the Field Extractor persist as knowledge objects is true. The Field Extractor (FX) is a graphical tool that allows you to extract fields from raw events using regular expressions or delimiters. The fields extracted by the FX are saved as knowledge objects that can be used in future searches or shared with other users.

NEW QUESTION 174

- (Exam Topic 2)

When a search returns _____, you can view the results as a list.

- A. a list of events
- B. transactions
- C. statistical values

Answer: C

NEW QUESTION 179

- (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 180

- (Exam Topic 2)

Complete the search, | _____ failure>successes

- A. Search
- B. Where
- C. If
- D. Any of the above

Answer: B

Explanation:

The where command can be used to complete the search below.

... | where failure>successes

The where command is a search command that allows you to filter events based on complex or custom criteria. The where command can use any boolean expression or function to evaluate each event and determine whether to keep it or discard it. The where command can also compare fields or perform calculations on fields using operators such as >, <, =, +, -, etc. The where command can be used after any transforming command that creates a table or a chart.

The search string below does the following:

- It uses ... to represent any search criteria or commands before the where command.
- It uses the where command to filter events based on a comparison between two fields: failure and successes.
- It uses the greater than operator (>) to compare the values of failure and successes fields for each event.
- It only keeps events where failure is greater than successes.

NEW QUESTION 183

- (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 188

- (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 191

- (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 193

- (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 197

- (Exam Topic 2)

Which of the following statements about tags is true? (select all that apply.)

- A. Tags are case-insensitive.
- B. Tags are based on field/value pairs.
- C. Tags categorize events based on a search.
- D. Tags are designed to make data more understandable.

Answer: BD

Explanation:

The following statements about tags are true: tags are based on field/value pairs and tags categorize events based on a search. Tags are custom labels that can be applied to fields or field values to provide additional context or meaning for your data. Tags can be used to filter or analyze your data based on common concepts or themes. Tags can be created by using various methods, such as search commands, configuration files, user interfaces, etc. Some of the characteristics of tags are:

> Tags are based on field/value pairs: This means that tags are associated with a specific field name and a specific field value. For example, you can create a tag called "alert" for the field name "status" and the field value "critical". This means that only events that have status=critical will have the "alert" tag applied to them.

> Tags categorize events based on a search: This means that tags are defined by a search string that matches the events that you want to tag. For example, you can create a tag called "web" for the search string sourcetype=access_combined. This means that only events that match the search string sourcetype=access_combined will have the "web" tag applied to them.

The following statements about tags are false: tags are case-insensitive and tags are designed to make data more understandable. Tags are case-sensitive and tags are designed to make data more searchable. Tags are case-sensitive: This means that tags must match the exact case of the field name and field value that they are associated with. For example, if you create a tag called "alert" for the field name "status" and the field value "critical", it will not apply to events that have status=CRITICAL or Status=critical. Tags are designed to make data more searchable: This means that tags can help you find relevant events or patterns in your data by using common concepts or themes. For example, if you create a tag called "web" for the search string sourcetype=access_combined, you can use tag=web to find all events related to web activity.

NEW QUESTION 201

- (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 205

- (Exam Topic 2)

Which of the following eval command functions is valid?

- A. int()
- B. count()
- C. print()
- D. tostring()

Answer: D

Explanation:

<https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/CommonEvalFunctions>

The eval command function tostring() is valid. The tostring() function converts a numeric value to a string value. For example, tostring(3.14) returns “3.14”. The other functions are not valid eval command functions.

NEW QUESTION 208

- (Exam Topic 2)

Which of the following searches would return a report of sales by product-name?

- A. chart sales by product_name
- B. chart sum(price) as sales by product_name
- C. stats sum(price) as sales over product_name
- D. timechart list(sales), values(product_name)

Answer: B

Explanation:

<https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/Chart> <https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/Stats>

NEW QUESTION 212

- (Exam Topic 2)

When using | timchart by host, which field is represented in the x-axis?

- A. date
- B. host
- C. time
- D. -time

Answer: A

NEW QUESTION 213

- (Exam Topic 2)

Which of the following is included with the Common Information Model (CIM) add-on?

- A. Search macros
- B. Event category tags
- C. Workflow actions
- D. tsidx files

Answer: B

Explanation:

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.

NEW QUESTION 216

- (Exam Topic 2)

These kinds of charts represent a series in a single bar with multiple sections

- A. Multi-Series
- B. Split-Series
- C. Omit nulls
- D. Stacked

Answer: D

Explanation:

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

NEW QUESTION 220

- (Exam Topic 2)

A data model consists of which three types of datasets?

- A. Constraint, field, value.
- B. Events, searches, transactions.
- C. Field extraction, regex, delimited.
- D. Transaction, session ID, metadata.

Answer: B

Explanation:

The building block of a data model. Each data model is composed of one or more data model datasets. Each dataset within a data model defines a subset of the dataset represented by the data model as a whole.

Data model datasets have a hierarchical relationship with each other, meaning they have parent-child relationships. Data models can contain multiple dataset hierarchies. There are three types of dataset hierarchies: event, search, and transaction.

<https://docs.splunk.com/Spdexicon:Datamodeldataset>

NEW QUESTION 223

- (Exam Topic 2)

Which of the following is one of the pre-configured data models included in the Splunk Common Information Model (CIM) add-on?

- A. Access
- B. Accounting
- C. Authorization
- D. Authentication

Answer: D

NEW QUESTION 227

- (Exam Topic 2)

When defining a macro, what are the required elements?

- A. Name and arguments.
- B. Name and a validation error message.
- C. Name and definition.
- D. Definition and arguments.

Answer: C

Explanation:

When defining a search macro, the required elements are the name and the definition of the macro. The name is a unique identifier for the macro that can be used to invoke it in other searches. The definition is the search string that the macro expands to when referenced. The arguments, validation expression, and validation error message are optional elements that can be used to customize the macro behavior and input validation²

1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, Define search macros in Settings.

NEW QUESTION 231

- (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 236

- (Exam Topic 2)

Which search would limit an "alert" tag to the "host" field?

- A. tag=alert
- B. host::tag::alert
- C. tag==alert
- D. tag::host=alert

Answer: D

Explanation:

The search below would limit an "alert" tag to the "host" field. tag::host=alert

The search does the following:

- It uses tag syntax to filter events by tags. Tags are custom labels that can be applied to fields or field values to provide additional context or meaning for your data.
- It specifies tag::host=alert as the tag filter. This means that it will only return events that have an "alert" tag applied to their host field or host field value.
- It uses an equal sign (=) to indicate an exact match between the tag and the field or field value.

NEW QUESTION 238

- (Exam Topic 2)

Which search string would only return results for an event type called success ful_purchases?

- A. tag=success ful_purchases
- B. Event Type:: successful purchases
- C. successful_purchases
- D. event type—success ful_purchases

Answer: C

Explanation:

This is because event types are added to events as a field named eventtype, and you can use this field as a search term to find events that match a specific event type. For example, eventtype=successful_purchases returns all events that have been categorized as successful purchases by the event type definition. The other options are incorrect because they either use a different field name (tag), a different syntax (Event Type:: or event type—), or have a typo (success ful_purchases). You can learn more about how to use event types in searches from the Splunk documentation¹.

NEW QUESTION 242

- (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 243

- (Exam Topic 2)

By default search results are not returned in _____ order.

- A. Chronological
- B. Reverser chronological
- C. ASCIE
- D. Alphabetical

Answer: AD

NEW QUESTION 246

- (Exam Topic 2)

Consider the following search: index=web sourcetype=access_corabined

The log shows several events that share the same jsessionid value (SD462K101O2F267). View the events as a group.

From the following list, which search groups events by jSESSIONID?

- A. index=web sourcetype=access_combined | transaction JSESSIONID | search SD462K101C2F267
- B. index=web sourcetype=access_combined SD462K101O2F267 | table JSESSIONID
- C. index=web sourcetype=access_combined | highlight JSESSIONID | search SD462K101O2F267
- D. index=web sourcetype=access_combined JSESSTONID <SD4€2K101O2F267>

Answer: A

Explanation:

The transaction command groups events that share a common value in a specified field, such as JSESSIONID, and that occur within a specified time range. The search command filters the results to show only the events that match the given value of JSESSIONID. This search groups the events by JSESSIONID and then shows only the events that have the value SD462K101C2F267 for JSESSIONID2

1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, transaction command.

NEW QUESTION 250

- (Exam Topic 2)

What is a limitation of searches generated by workflow actions?

- A. Searches generated by workflow action cannot use macros.
- B. Searches generated by workflow actions must be less than 256 characters long.
- C. Searches generated by workflow action must run in the same app as the workflow action.
- D. Searches generated by workflow action run with the same permissions as the user running them.

Answer: D

NEW QUESTION 255

- (Exam Topic 2)

It is mandatory for the lookup file to have this for an automatic lookup to work.

- A. Source type
- B. At least five columns
- C. Timestamp
- D. Input filed

Answer: D

NEW QUESTION 260

- (Exam Topic 2)

Which is not a comparison operator in Splunk

- A. <=
- B. =
- C. !=
- D. >
- E. ?=

Answer: E

Explanation:

A comparison operator is a symbol that compares two values and returns a Boolean result (true or

false)2. Splunk supports various comparison operators such as <, >, =, !=, <=, >=, IN and LIKE2. However, ?= is not a valid comparison operator in Splunk and will cause a syntax error if used in a search string2. Therefore, option E is correct, while options A, B, C and D are incorrect because they are valid comparison operators in Splunk

NEW QUESTION 262

- (Exam Topic 2)

There are several ways to access the field extractor. Which option automatically identifies data type, source type, and sample event?

- A. Event Actions > Extract Fields
- B. Fields sidebar > Extract New Field
- C. Settings > Field Extractions > New Field Extraction
- D. Settings > Field Extractions > Open Field Extraction

Answer: B

Explanation:

There are several ways to access the field extractor. The option that automatically identifies data type, source type, and sample event is Fields sidebar > Extract New Field. The field extractor is a tool that helps you extract fields from your data using delimiters or regular expressions. The field extractor can generate a regex for you based on your selection of sample values or you can enter your own regex in the field extractor. The field extractor can be accessed by using various methods, such as:

- Fields sidebar > Extract New Field: This is the easiest way to access the field extractor. The fields sidebar is a panel that shows all available fields for your data and their values. When you click on Extract New Field in the fields sidebar, Splunk will automatically identify the data type, source type, and sample event for your data based on your current search criteria. You can then use the field extractor to select sample values and generate a regex for your new field.
- Event Actions > Extract Fields: This is another way to access the field extractor. Event actions are actions that you can perform on individual events in your search results, such as viewing event details, adding to report, adding to dashboard, etc. When you click on Extract Fields in the event actions menu, Splunk will use the current event as the sample event for your data and ask you to select the source type and data type for your data. You can then use the field extractor to select sample values and generate a regex for your new field.
- Settings > Field Extractions > New Field Extraction: This is a more advanced way to access the field extractor. Settings is a menu that allows you to configure various aspects of Splunk, such as indexes, inputs, outputs, users, roles, apps, etc. When you click on New Field Extraction in the Settings menu, Splunk will ask you to enter all the details for your new field extraction manually, such as app context, name, source type, data type, sample event, regex, etc. You can then use the field extractor to verify or modify your regex for your new field.

NEW QUESTION 265

- (Exam Topic 2)

Which knowledge Object does the Splunk Common Information Model (CIM) use to normalize data. in addition to field aliases, event types, and tags?

- A. Macros
- B. Lookups
- C. Workflow actions
- D. Field extractions

Answer: B

Explanation:

Normalize your data for each of these fields using a combination of field aliases, field extractions, and lookups.
<https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsearchtime>

NEW QUESTION 269

- (Exam Topic 2)

This function of the stats command allows you to identify the number of values a field has.

- A. max
- B. distinct_count
- C. fields
- D. count

Answer: D

NEW QUESTION 272

- (Exam Topic 2)

What does the fillnull command replace null values with, if the value argument is not specified?

- A. N/A
- B. NaN
- C. NULL

Answer: A

Explanation:

The fillnull command replaces null values with 0 by default, if the value argument is not specified. You can use the value argument to specify a different value to replace null values with, such as N/A or NULL.

NEW QUESTION 277

- (Exam Topic 2)

The timechart command buckets data in time intervals depending on:

- A. the number of events returned

- B. the selected time range
- C. the type of visualization selected

Answer: B

Explanation:

The timechart command buckets data in time intervals depending on the selected time range². The timechart command is similar to the chart command but it automatically groups events into time buckets based on the _time field². The size of the time buckets depends on the time range that you select for your search. For example, if you select Last 24 hours as your time range, Splunk will use 30-minute buckets for your timechart. If you select Last 7 days as your time range, Splunk will use 4-hour buckets for your timechart². Therefore, option B is correct, while options A and C are incorrect because they are not factors that affect the size of the time buckets.

NEW QUESTION 281

- (Exam Topic 2)

Which of the following is a function of the Splunk Common Information Model (CIM)?

- A. Normalizing data across a Splunk deployment.
- B. Providing templates for reports and dashboards.
- C. Algorithmically shifting events to other indexes.
- D. Reingesting previously indexed data with new field names.

Answer: A

NEW QUESTION 282

- (Exam Topic 2)

Which statement is true?

- A. Pivot is used for creating datasets.
- B. Data models are randomly structured datasets.
- C. Pivot is used for creating reports and dashboards.
- D. In most cases, each Splunk user will create their own data model.

Answer: C

Explanation:

The statement that pivot is used for creating reports and dashboards is true. Pivot is a graphical interface that allows you to create tables, charts, and visualizations from data models. Data models are structured datasets that define how data is organized and categorized. Pivot does not create datasets, but uses existing ones.

NEW QUESTION 284

- (Exam Topic 2)

The stats command will create a _____ by default.

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

Answer: A

NEW QUESTION 286

- (Exam Topic 2)

Use the dedup command to _____.

- A. Rename a field in the index
- B. remove duplicate values
- C. provide an additional alias for the field that can
- D. be used in the search criteria

Answer: B

NEW QUESTION 287

- (Exam Topic 2)

Which syntax will find events where the values for the 1 field match the values for the Renewal-MonthYear field?

- A. | where 10yearAnniversary=Renewal-MonthYear
- B. | where '10yearAnniversary=Renewal-MonthYear
- C. | where 10yearAnniversary='Renewal-MonthYear'
- D. | where '10yearAnniversary'='Renewal-MonthYear'

Answer: A

Explanation:

The correct answer is A. | where 10yearAnniversary=Renewal-MonthYear.

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 10yearAnniversary field match the values for the Renewal-MonthYear field, you can use the following syntax:

| where 10yearAnniversary=Renewal-MonthYear

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

The other options are not correct because they use quotation marks around the field names, which will cause the where command to interpret them as string values instead of field names. For example, if you use:

| where '10yearAnniversary'='Renewal-MonthYear'

This will return no events because there are no events where the string value '10yearAnniversary' is equal to the string value 'Renewal-MonthYear'.

References:

➤ [where command usage](#)

NEW QUESTION 290

- (Exam Topic 2)

Which of the following transforming commands can be used with transactions?

- A. chart, timechart, stats, eventstats
- B. chart, timechart, stats, diff
- C. chart, timechart, datamodel, pivot
- D. chart, timechart, stats, pivot

Answer: A

Explanation:

The correct answer is A. chart, timechart, stats, eventstats.

Transforming commands are commands that change the format of the search results into a table or a chart. They can be used to perform statistical calculations, create visualizations, or manipulate data in various ways¹.

Transactions are groups of events that share some common values and are related in some way. Transactions can be defined by using the transaction command or by creating a transaction type in the transactiontypes.conf file².

Some transforming commands can be used with transactions to create tables or charts based on the transaction fields. These commands include:

➤ chart: This command creates a table or a chart that shows the relationship between two or more fields. It can be used to aggregate values, count occurrences, or calculate statistics³.

➤ timechart: This command creates a table or a chart that shows how a field changes over time. It can be used to plot trends, patterns, or outliers⁴.

➤ stats: This command calculates summary statistics on the fields in the search results, such as count, sum, average, etc. It can be used to group and aggregate data by one or more fields⁵.

➤ eventstats: This command calculates summary statistics on the fields in the search results, similar to stats, but it also adds the results to each event as new fields. It can be used to compare events with the overall statistics.

These commands can be applied to transactions by using the transaction fields as arguments. For example, if you have a transaction type named "login" that groups events based on the user field and has fields such as duration and eventcount, you can use the following commands with transactions:

➤ | chart count by user : This command creates a table or a chart that shows how many transactions each user has.

➤ | timechart span=1h avg(duration) by user : This command creates a table or a chart that shows the average duration of transactions for each user per hour.

➤ | stats sum(eventcount) as total_events by user : This command creates a table that shows the total number of events for each user across all transactions.

➤ | eventstats avg(duration) as avg_duration : This command adds a new field named avg_duration to each transaction that shows the average duration of all transactions.

The other options are not valid because they include commands that are not transforming commands or cannot be used with transactions. These commands are:

➤ diff: This command compares two search results and shows the differences between them. It is not a transforming command and it does not work with transactions.

➤ datamodel: This command retrieves data from a data model, which is a way to organize and categorize data in Splunk. It is not a transforming command and it does not work with transactions.

➤ pivot: This command creates a pivot report, which is a way to analyze data from a data model using a graphical interface. It is not a transforming command and it does not work with transactions.

References:

➤ [About transforming commands](#)

➤ [About transactions](#)

➤ [chart command overview](#)

➤ [timechart command overview](#)

➤ [stats command overview](#)

➤ [\[eventstats command overview\]](#)

➤ [\[diff command overview\]](#)

➤ [\[datamodel command overview\]](#)

➤ [\[pivot command overview\]](#)

NEW QUESTION 293

- (Exam Topic 2)

The eval command allows you to do which of the following? (Choose all that apply.)

- A. Format values
- B. Convert values
- C. Perform calculations
- D. Use conditional statements

Answer: ABCD

NEW QUESTION 296

- (Exam Topic 2)

Which tool uses data models to generate reports and dashboard panels without using SPL?

- A. Visualization tab
- B. Pivot
- C. Datasets
- D. splunk CIM

Answer: B

Explanation:

The correct answer is B. Pivot1.

In Splunk, Pivot is a tool that uses data models to generate reports and dashboard panels without the need for users to write or understand Splunk's Search Processing Language (SPL)1. Data models enable users of Pivot to create compelling reports and dashboards1. When a Pivot user designs a pivot report, they select the data model that represents the category of event data that they want to work with1. Then they select a dataset within that data model that represents the specific dataset on which they want to report1. This makes Pivot a powerful tool for users who need to create visualizations but do not have a deep understanding of SPL1.

NEW QUESTION 297

- (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 301

- (Exam Topic 2)

Which workflow action type performs a secondary search?

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

Answer: D

Explanation:

The correct answer is D. Search.

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 workflow action type that performs a secondary search is Search. References:

- [Splexicon:Workflowaction](#)
- [About workflow actions in Splunk Web](#)

NEW QUESTION 303

- (Exam Topic 2)

When used with the timechart command, which value of the limit argument returns all values?

- A. limit=*
- B. limit=all
- C. limit=none
- D. limit=0

Answer: D

Explanation:

The correct answer is D. limit=0. This is because the limit argument specifies the maximum number of series to display in the chart. If you set limit=0, no series filtering occurs and all values are returned. You can learn more about the limit argument and how it works with the agg argument from the Splunk documentation1.

The other options are incorrect because they are not valid values for the limit argument. The limit argument expects an integer value, not a string or a wildcard.

You can learn more about the syntax and usage of the timechart command from the Splunk documentation23.

NEW QUESTION 305

- (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 308

- (Exam Topic 2)

Which workflow uses field values to perform a secondary search?

- A. POST
- B. Action
- C. Search
- D. Sub-Search

Answer: C

Explanation:

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

NEW QUESTION 310

- (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 311

- (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"))
```

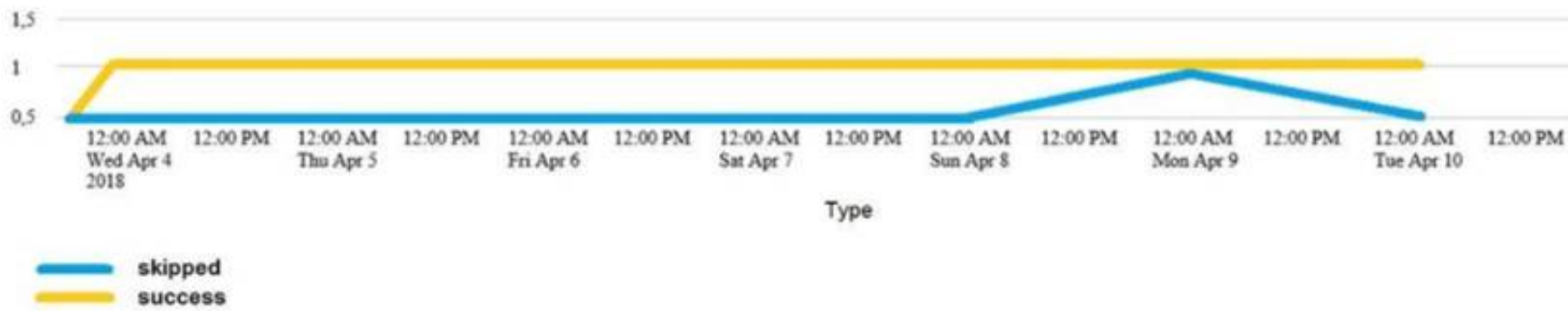
This will expand the macros with the corresponding arguments and run the SPL code contained in them. References:

- [Search macro examples](#)
- [Use search macros in searches](#)

NEW QUESTION 312

- (Exam Topic 2)

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



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

Answer: C

Explanation:

The following search would create a graph similar to the one below:

index_internal sourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan=1d | timechart count by status

The search does the following:

- > It uses index_internal to specify the internal index that contains Splunk logs and metrics.
- > It uses sourcetype=Savesplunker to filter events by the sourcetype that indicates the Splunk Enterprise Security app.
- > It uses fields sourcetype, status to keep only the sourcetype and status fields in the events.
- > It uses transaction status maxspan=1d to group events into transactions based on the status field with a maximum time span of one day between the first and last events in a transaction.
- > It uses timechart count by status to create a time-based chart that shows the count of transactions for each status value over time.

The graph shows the following:

- > It is a line graph with two lines, one yellow and one blue.
- > The x-axis is labeled with dates from Wed, Apr 4, 2018 to Tue, Apr 10, 2018.
- > The y-axis is labeled with numbers from 0 to 15.
- > The yellow line represents "shipped" and the blue line represents "success".
- > The yellow line has a steady increase from 0 to 15, while the blue line has a sharp increase from 0 to 5, then a decrease to 0, and then a sharp increase to 10.
- > The graph is titled "Type". Therefore, option C is the correct answer.

NEW QUESTION 315

- (Exam Topic 2)

Which of the following is true about the Splunk Common Information Model (CIM)?

- A. The data models included in the CIM are configured with data model acceleration turned off.
- B. The CIM contains 28 pre-configured datasets.
- C. The CIM is an app that needs to run on the indexer.
- D. The data models included in the CIM are configured with data model acceleration turned on.

Answer: D

Explanation:

The Splunk Common Information Model (CIM) is an app that contains a set of predefined data models that apply a common structure and naming convention to data from any source. The CIM enables you to use data from different sources in a consistent and coherent way. The CIM contains 28 pre-configured datasets that cover various domains such as authentication, network traffic, web, email, etc. The data models included in the CIM are configured with data model acceleration turned on by default, which means that they are optimized for faster searches and analysis. Data model acceleration creates and maintains summary data for the data models, which reduces the amount of raw data that needs to be scanned when you run a search using a data model.

Splunk Core Certified Power User Track, page 10. : Splunk Documentation, About the Splunk Common Information Model.

NEW QUESTION 319

- (Exam Topic 2)

In the following eval statement, what is the value of description if the status is 503? index=main | eval description=case(status==200, "OK", status==404, "Not found", status==500, "Internal Server Error")

- A. The description field would contain no value.
- B. The description field would contain the value 0.
- C. The description field would contain the value "Internal Server Error".
- D. This statement would produce an error in Splunk because it is incomplete.

Answer: A

Explanation:

<https://docs.splunk.com/Documentation/Splunk/8.1.1/SearchReference/ConditionalFunctions>

NEW QUESTION 322

- (Exam Topic 2)

Why would the following search produce multiple transactions instead of one?


```
index=security sourcetype=linux_secure failed earliest=-60d@d latest=-1d@d
| transaction src_ip
| stats list(eventcount) as num_events sum(eventcount) as total_events by src_ip
```

Events (641) Patterns **Statistics (147)** Visualization

20 Per Page ▾ / Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 Next >

src	num_events	total_events
107.3.146.207	1000 1000 1000 405	3405
108.65.113.83	1000 120	1120
109.169.32.135	1000 1000 79	2079
11.17.160.129	1000 1000 238	2238

- A. The maxspan option is not included.
- B. The transaction command has a limit of 1000 events per transaction.
- C. The transaction and commands cannot be used together.
- D. The stats list () function is used.

Answer: A

Explanation:

The correct answer is A. The maxspan option is not included1.

In Splunk, the transaction command is used to group events that share common characteristics into a single transaction1. By default, the transaction command groups all matching events into a single transaction1.

However, you can use the maxspan option to limit the time span of the transactions1. If the time span between the first and last event in a transaction exceeds the maxspan value, the transaction command will start a new transaction1.

Therefore, if the maxspan option is not included in the search, the transaction command might produce multiple transactions instead of one if the time span between the first and last event in a transaction exceeds the default maxspan value1.

Here is an example of how you can use the maxspan option in a search:

```
index=main sourcetype=access_combined | transaction someuniquefield maxspan=1h
```

In this search, the transaction command groups events that share the same someuniquefield value into a single transaction, but only if the time span between the first and last event in the transaction does not exceed 1 hour1. If the time span exceeds 1 hour, the transaction command will start a new transaction1.

NEW QUESTION 323

- (Exam Topic 2)

Which of the following searches will return all clientip addresses that start with 108?

- A. ... | where like (clientip, "108.%")
- B. ... | where (clientip, "108. %")
- C. ... | where (clientip=108. %)
- D. ... | search clientip=108

Answer: A

NEW QUESTION 326

- (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 330

- (Exam Topic 2)

During the validation step of the Field Extractor workflow: Select your answer.

- A. You can remove values that aren't a match for the field you want to define
- B. You can validate where the data originated from
- C. You cannot modify the field extraction

Answer: A

Explanation:

During the validation step of the Field Extractor workflow, you can remove values that aren't a match for the field you want to define². The validation step allows you to review and edit the values that have been extracted by the FX and make sure they are correct and consistent². You can remove values that aren't a match by clicking on them and selecting Remove Value from the menu². This will exclude them from your field extraction and update the regular expression accordingly². Therefore, option A is correct, while options B and C are incorrect because they are not actions that you can perform during the validation step of the Field Extractor workflow.

NEW QUESTION 333

- (Exam Topic 2)

Splunk alerts can be based on search that run _____. (Select all that apply.)

- A. in real-time
- B. on a regular schedule
- C. and have no matching events

Answer: AB

Explanation:

Splunk alerts can be based on searches that run in real-time or on a regular schedule³. An alert is a way to monitor your data and get notified when certain conditions are met³. You can create an alert by specifying a search and a triggering condition³. You can also specify how often you want to run the search and how you want to receive the alert notifications³. You can run the alert search in real-time, which means that it continuously monitors your data as it streams into Splunk³. Alternatively, you can run the alert search on a regular schedule, which means that it runs at fixed intervals such as every hour or every day³. Therefore, options A and B are correct, while option C is incorrect because it is not a way to run an alert search.

NEW QUESTION 337

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SPLK-1002 Practice Exam Features:

- * SPLK-1002 Questions and Answers Updated Frequently
- * SPLK-1002 Practice Questions Verified by Expert Senior Certified Staff
- * SPLK-1002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SPLK-1002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SPLK-1002 Practice Test Here](#)