

Splunk

Exam Questions SPLK-1002

Splunk Core Certified Power User Exam



NEW QUESTION 1

- (Exam Topic 1)

A space is an implied _____ in a search string.

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

Answer: B

Explanation:

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

NEW QUESTION 2

- (Exam Topic 1)

Which of the following statements 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 3

- (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 4

- (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 5

- (Exam Topic 1)

Which of the following can be used with the eval command tostring function (select all that apply)

- A. "hex"
- B. "commas"
- C. "Decimal"
- D. "duration"

Answer: ABD

Explanation:

<https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/ConversionFunctions#tostring.28X.2CY> The tostring function in the eval command converts a numeric value to a string value. It can take an optional second argument that specifies the format of the string value. Some of the possible formats are:

- hex: converts the numeric value to a hexadecimal string.
- commas: adds commas to separate thousands in the numeric value.
- duration: converts the numeric value to a human-readable duration string, such as "2h 3m 4s". Therefore, the formats A, B, and D can be used with the tostring function.

NEW QUESTION 6

- (Exam Topic 1)

Which of the following statements describes macros?

- A. A macro is a reusable search string that must contain the full search.
- B. A macro is a reusable search string that must have a fixed time range.
- C. A macro is a reusable search string that may have a flexible time range.
- D. A macro is a reusable search string that must contain only a portion of the search.

Answer: C

Explanation:

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

A macro is a reusable search string that can contain any part of a search, such as search terms, commands, arguments, etc. A macro can have a flexible time range that can be specified when the macro is executed. A macro can also have arguments that can be passed to the macro when it is executed. A macro can be created by using the Settings menu or by editing the macros.conf file. A macro does not have to contain the full search, but only the part that needs to be reused. A macro does not have to have a fixed time range, but can use a relative or absolute time range modifier. A macro does not have to contain only a portion of the search, but can contain multiple parts of the search.

NEW QUESTION 7

- (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 8

- (Exam Topic 1)

Which of the following statements about data models and pivot are true? (select all that apply)

- A. They are both knowledge objects.
- B. Data models are created out of datasets called pivots.
- C. Pivot requires users to input SPL searches on data models.
- D. Pivot allows the creation of data visualizations that present different aspects of a data model.

Answer: D

Explanation:

Data models and pivot are both knowledge objects in Splunk that allow you to analyze and visualize your data in different ways. Data models are collections of datasets that represent your data in a structured and hierarchical way. Data models define how your data is organized into objects and fields. Pivot is a user interface that allows you to create data visualizations that present different aspects of a data model. Pivot does not require users to input SPL searches on data models, but rather lets them select options from menus and forms. Data models are not created out of datasets called pivots, but rather pivots are created from datasets in data models.

NEW QUESTION 9

- (Exam Topic 1)

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

Destination app
oidemo

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

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

☐ Use eval-based definition?

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

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

Answer: B

Explanation:

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

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

sessiontracker(2)

The macro definition does the following:

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

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

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

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

NEW QUESTION 10

- (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 10

- (Exam Topic 1)

In what order are the following knowledge objects/configurations applied?

- A. Field Aliases, Field Extractions, Lookups
 B. Field Extractions, Field Aliases, Lookups
 C. Field Extractions, Lookups, Field Aliases
 D. Lookups, Field Aliases, Field Extractions

Answer: B

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/WhatisSplunkknowledge> Knowledge objects are entities that you create to add knowledge to your data and make it easier to search and analyze2. Some examples of knowledge objects are field extractions, field aliases and lookups2. Field extractions are methods that extract fields from your raw data using various techniques such as regular expressions, delimiters or key-value pairs2. Field aliases are ways to assign alternative names to existing fields without changing the original field names or values2. Lookups are ways to enrich your data with additional information from external sources such as CSV files or databases2. The order in which these knowledge objects/configurations are applied is as follows: field extractions, field aliases and then lookups2. This means that Splunk first extracts fields from your raw data, then applies any aliases to the extracted fields and then performs any lookups on the aliased fields2. Therefore, option B is correct, while options A, C and D are incorrect.

NEW QUESTION 15

- (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 REJECT². 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 19

- (Exam Topic 1)

What functionality does the Splunk Common Information Model (CIM) rely on to normalize fields with different names?

- A. Macros.
- B. Field aliases.
- C. The rename command.
- D. CIM does not work with different names for the same field.

Answer: B

Explanation:

The Splunk Common Information Model (CIM) add-on helps you normalize your data from different sources and make it easier to analyze and report on it³. One of the functionalities that the CIM add-on relies on to normalize fields with different names is field aliases³. Field aliases allow you to assign an alternative name to an existing field without changing the original field name or value². By using field aliases, you can map different field names from different sources or sourcetypes to a common field name that conforms to the CIM standard³. Therefore, option B is correct, while options A, C and D are incorrect.

NEW QUESTION 20

- (Exam Topic 1)

Which of the following statements describes this search? sourcetype=access_combined | transaction JSESSIONID | timechart avg (duration)

- A. This is a valid search and will display a timechart of the average duration, of each transaction event.
- B. This is a valid search and will display a stats table showing the maximum pause among transactions.
- C. No results will be returned because the transaction command must include the startswith and endswith options.
- D. No results will be returned because the transaction command must be the last command used in the search pipeline.

Answer: A

Explanation:

This search uses the transaction command to group events that share a common value for JSESSIONID into transactions¹. The transaction command assigns a duration field to each transaction, which is the difference between the latest and earliest timestamps of the events in the transaction¹. The search then uses the timechart command to create a time-series chart of the average duration of each transaction¹. Therefore, option A is correct because it describes the search accurately. Option B is incorrect because the search does not use the stats command or the pause field. Option C is incorrect because the transaction command does not require the startswith and endswith options, although they can be used to specify how to identify the beginning and end of a transaction¹. Option D is incorrect because the transaction command does not have to be the last command in the search pipeline, although it is often used near the end of a search¹.

NEW QUESTION 23

- (Exam Topic 1)

Which delimiters can the Field Extractor (FX) detect? (select all that apply)

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

Answer: BCD

Explanation:

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

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. The FX can detect some common delimiters automatically, such as pipes (|), spaces (), commas (,), semicolons (;), etc. The FX cannot detect tabs (\t) as delimiters automatically, but you can specify them manually in the FX interface.

NEW QUESTION 26

- (Exam Topic 1)

Which of the following eval command function is valid?

- A. Int ()
- B. Count ()

- C. Print ()
- D. ToString ()

Answer: D

Explanation:

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

NEW QUESTION 27

- (Exam Topic 1)

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

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

Answer: ACD

Explanation:

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

As mentioned before, an event type is a way to categorize events based on a search string that matches the events². Event types can be tagged, which means that you can apply descriptive labels to event types and use them in your searches². Therefore, option A is correct. Event types categorize events based on a search string, which means that you can define an event type by specifying a search string that matches the events you want to include in the event type².

Therefore, option C is correct. Event types can be a useful method for capturing and sharing knowledge, which means that you can use event types to organize your data into meaningful categories and share them with other users in your organization². Therefore, option D is correct. Event types do not have to include a time range, which means that you can create an event type without specifying a time range for the events². Therefore, option B is incorrect.

NEW QUESTION 28

- (Exam Topic 1)

Which one of the following statements about the search command is true?

- A. It does not allow the use of wildcards.
- B. It treats field values in a case-sensitive manner.
- C. It can only be used at the beginning of the search pipeline.
- D. It behaves exactly like search strings before the first pipe.

Answer: D

Explanation:

Reference: <https://docs.splunk.com/Documentation/SplunkCloud/8.0.2003/Search/Usetheseearchcommand> The search command is used to filter or refine your search results based on a search string that matches the events². The search command behaves exactly like search strings before the first pipe, which means that you can use the same syntax and operators as you would use in the initial part of your search². Therefore, option D is correct, while options A, B and C are incorrect because they are not true statements about the search command.

NEW QUESTION 33

- (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 38

- (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/Setupsearchworkflowaction> 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 40

- (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 43

- (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 45

- (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 47

- (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 49

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 54

- (Exam Topic 2)

When using the transaction command, how are evicted transactions identified?

- A. Closed_txn field is set to 0, or false.
- B. Max_txn field is set to 0, or false.
- C. Txn_field is set to 1, or true.
- D. open_txn field is set to 1, or true.

Answer: A

Explanation:

- The transaction command is a Splunk command that finds transactions based on events that meet various constraints¹.
- Transactions are made up of the raw text (the _raw field) of each member, the time and date fields of the earliest member, as well as the union of all other fields of each member¹.
- The transaction command adds some fields to the raw events that are part of the transaction¹². These fields are:
 - duration: The difference, in seconds, between the timestamps for the first and last events in the transaction¹².
 - eventcount: The number of events in the transaction¹².
 - closed_txn: A Boolean field that indicates whether the transaction is closed or evicted². A transaction is closed if it meets one of the following conditions: maxevents, maxpause, maxsp or startswith². A transaction is evicted if it does not meet any of these conditions and exceeds the memory limit specified by maxopentxn or maxopenevents²³.
- Therefore, evicted transactions can be distinguished from non-evicted transactions by checking the value of the closed_txn field. The closed_txn field is set to 0, or false, for evicted transactions and 1 for non-evicted, or closed, transactions²³.

NEW QUESTION 56

- (Exam Topic 2)

Which of the following search control will not re-run 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 58

- (Exam Topic 2)

Which field extraction method should be selected for comma-separated data?

- A. Regular expression
- B. Delimiters
- C. eval expression
- D. table extraction

Answer: B

Explanation:

The correct answer is B. Delimiters. This is because the delimiters method is designed for structured event data, such as data from files with headers, where all of the fields in the events are separated by a common delimiter, such as a comma or space. You can select a sample event, identify the delimiter, and then rename the fields that the field extractor finds. You can learn more about the delimiters method from the Splunk documentation¹. The other options are incorrect because they are not suitable for comma-separated data. The regular expression method works best with unstructured event data, where you select and highlight one or

more fields to extract from a sample event, and the field extractor generates a regular expression that matches similar events and extracts the fields from them. The eval expression is a command that lets you calculate new fields or modify existing fields using arithmetic, string, and logical operations. The table extraction is a feature that lets you extract tabular data from PDF files or web pages. You can learn more about these methods from the Splunk documentation²³.

NEW QUESTION 59

- (Exam Topic 2)

Using the export function, you can export search results as _____. (Select all that apply)

- A. Xml
- B. Json
- C. Html
- D. A php file

Answer: AB

Explanation:

Using the export function, you can export search results as XML or JSON². The export function allows you to save your search results in a structured format that can be used by other applications or tools². You can use the output_mode parameter to specify whether you want to export your results as XML or JSON². Therefore, options A and B are correct, while options C and D are incorrect because they are not formats that you can export your search results as.

NEW QUESTION 62

- (Exam Topic 2)

We can use the rename command to _____ (Select all that apply.)

- A. Change indexed fields
- B. Exclude fields from our search results
- C. Extract new fields from our data using regular expressions
- D. Give a field a new name at search time

Answer: D

NEW QUESTION 66

- (Exam Topic 2)

When can a pipe follow a macro?

- A. A pipe may always follow a macro.
- B. The current user must own the macro.
- C. The macro must be defined in the current app.
- D. Only when sharing is set to global for the macro.

Answer: A

Explanation:

A macro is a way to save a segment of a search string as a variable and reuse it in other searches². A macro can be followed by a pipe, which is a symbol that separates commands in a search pipeline². A pipe may always follow a macro, regardless of who owns the macro, where the macro is defined or how the macro is shared². For example, if you have a macro called us_sales that returns events from the US region, you can use it in a search like this: us_sales | stats sum(price) by product². This search will use the macro to filter the events and then calculate the total price for each product². Therefore, option A is correct, while options B, C and D are incorrect because they are not conditions that affect whether a pipe can follow a macro.

NEW QUESTION 69

- (Exam Topic 2)

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

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

Answer: ABC

Explanation:

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

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

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

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

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

NEW QUESTION 70

- (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 75

- (Exam Topic 2)

A data model can consist of what three types of datasets?

- A. Pivot, searches, and events.
- B. Pivot, events, and transactions.
- C. Searches, transactions, and pivot.
- D. Events, searches, and transactions.

Answer: D

NEW QUESTION 77

- (Exam Topic 2)

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

- A. inputlookup
- B. lookup

Answer: B

NEW QUESTION 78

- (Exam Topic 2)

The macro weekly_sales (2) contains the search string:

index—games | eval Product Sales = \$price\$ \$Amount\$01d\$ Which of the following will return results?

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

Answer: C

Explanation:

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

NEW QUESTION 79

- (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 83

- (Exam Topic 2)

How are event types different from saved reports?

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

Answer: D

Explanation:

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

The explanation is as follows:

➤ Event types are a categorization system that help you make sense of your data by matching events with the same search string¹. Event types are applied to

events at search time and can be used as search terms or filters¹².

- Saved reports are results saved from a search action that can show statistics and visualizations of events³. Saved reports can be run anytime, and they fetch fresh results each time they are run³⁴. Saved reports can be shared with other users and added to dashboards⁴.
- The main difference between event types and saved reports is that event types do not include a time range, while saved reports do¹⁴. This means that event types can match events from any time period, while saved reports are limited by the time range specified when they are created or run¹⁴.

NEW QUESTION 86

- (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 90

- (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 91

- (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 96

- (Exam Topic 2)

What are search macros?

- A. Lookup definitions in lookup tables.
- B. Reusable pieces of search processing language.
- C. A method to normalize fields.
- D. Categories of search results.

Answer: B

Explanation:

The correct answer is B. Reusable pieces of search processing language. The explanation is as follows:

- Search macros are knowledge objects that allow you to insert chunks of SPL into other searches¹².
- Search macros can be any part of a search, such as an eval statement or a search term, and do not need to be a complete command¹².
- You can also specify whether the macro field takes any arguments and define validation expressions for them¹².
- Search macros can help you make your SPL searches shorter and easier to understand³.
- To use a search macro in a search string, you need to put a backtick character (`) before and after the macro name^{[^1^][1]}. For example, mymacro`.

NEW QUESTION 100

- (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_name
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 command

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

NEW QUESTION 105

- (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 107

- (Exam Topic 2)

Which of the following statements describes calculated fields?

- A. Calculated fields are only used on fields added by lookups.
- B. Calculated fields are a shortcut for repetitive and complex eval commands.
- C. Calculated fields are a shortcut for repetitive and complex calc commands.
- D. Calculated fields automatically calculate the simple moving average for indexed fields.

Answer: B

NEW QUESTION 111

- (Exam Topic 2)

Which method in the Field Extractor would extract the port number from the following event?

| 10/20/2022 - 125.24.20.1 ++++ port 54 - user: admin <web error>

- A. Delimiter
- B. rex command
- C. The Field Extractor tool cannot extract regular expressions.
- D. Regular expression

Answer: B

Explanation:

The rex command allows you to extract fields from events using regular expressions. You can use the rex command to specify a named group that matches the port number in the event. For example:

```
rex "\+\\+\\+port (?<port>\\d+)"
```

This will create a field called port with the value 54 for the event.

The delimiter method is not suitable for this event because there is no consistent delimiter between the fields. The regular expression method is not a valid option for the Field Extractor tool. The Field Extractor tool can extract regular expressions, but it is not a method by itself.

Reference: 1

Splunk Core Certified Power User | Splunk

NEW QUESTION 112

- (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 114

- (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 117

- (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 120

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

with information from an event.

NEW QUESTION 123

- (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 128

- (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 129

- (Exam Topic 2)

Which of the following searches show a valid use of a macro? (Choose all that apply.)

- A. index=main source=mySource oldField=* |'makeMyField(oldField)'| table _time newField
- B. index=main source=mySource oldField=* | stats if('makeMyField(oldField)') | table _time newField
- C. index=main source=mySource oldField=* | eval newField='makeMyField(oldField)'| table _time newField
- D. index=main source=mySource oldField=* | "newField('makeMyField(oldField)')"' | table _time newField

Answer: AC

Explanation:

The searches A and C show a valid use of a macro. A macro is a reusable piece of SPL code that can be called by using single quotes ('). A macro can take arguments, which are passed inside parentheses after the macro name. For example, 'makeMyField(oldField)' calls a macro named makeMyField with an argument oldField. The searches B and D are not valid because they use double quotes (") instead of single quotes (').

NEW QUESTION 131

- (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 133

- (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 138

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 139

- (Exam Topic 2)

Why are tags useful in Splunk?

- A. Tags look for less specific data.
- B. Tags visualize data with graphs and charts.
- C. Tags group related data together.
- D. Tags add fields to the raw event data.

Answer: C

Explanation:

Tags are a type of knowledge object that enable you to assign descriptive keywords to events based on the values of their fields. Tags can help you to search more efficiently for groups of event data that share common characteristics, such as functionality, location, priority, etc. For example, you can tag all the IP addresses of your routers as router, and then search for tag=router to find all the events related to your routers. Tags can also help you to normalize data from different sources by using the same tag name for equivalent field values. For example, you can tag the field values error, fail, and critical as severity=high, and then search for severity=high to find all the events with high severity level²

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

NEW QUESTION 144

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

A workflow action is a knowledge object that enables a variety of interactions between fields in events and other web resources. Workflow actions can create

HTML links, generate HTTP POST requests, or launch secondary searches based on field values¹.

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

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

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

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

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

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

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

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

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

References:

➤ Splxicon:Workflowaction

➤ About workflow actions in Splunk Web

NEW QUESTION 149

- (Exam Topic 2)

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

A. Calculated fields cannot be chained together to create more complex fields

B. Calculated fields can be chained together to create more complex fields.

C. Calculated fields can only be used in dashboards.

D. Calculated fields can only be used in saved reports.

Answer: B

Explanation:

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

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

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

discount = total * 0.9

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

➤ About calculated fields

➤ Chaining calculated fields

NEW QUESTION 154

- (Exam Topic 2)

How is an event type created from the search window? (select all that apply)

A. In the top right corner, click Save As > Event Type.

B. In an event's detail dropdown, click Event Actions > Build Event Type.

C. Edit eventtypes.conf and add a new stanza.

D. Add | eventtype to the SPL and execute the search.

Answer: AC

Explanation:

In Splunk, you can create an event type from the search window by running a search that would make a good event type, then clicking Save As and selecting Event Type¹. This opens the Save as Event Type dial you can provide the event type name and optionally apply tags to it¹.

You can also create an event type by editing the eventtypes.conf file and adding a new stanza¹. Each stanza in the eventtypes.conf file represents an event type¹.

The stanza name is the name of the event type, and

the search attribute specifies the search string that defines the event type¹.

It's important to note that while you can use the eventtype command in a search to find events associated with a specific event type, adding | eventtype to the SPL and executing the search does not create a new event type¹. Similarly, clicking Event Actions > Build Event Type in an event's detail dropdown does not create new event type¹.

NEW QUESTION 155

- (Exam Topic 2)

These users can create global knowledge objects. (Select all that apply.)

A. users

B. power users

C. administrators

Answer: BC

NEW QUESTION 157

- (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 159

- (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 160

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 163

- (Exam Topic 2)

If a calculated field has the same name as an extracted field, what happens to the extracted field?

- A. The calculated field will override the extracted field.
- B. The calculated and extracted fields will be combined.
- C. The calculated field will duplicate the extracted field.
- D. An error will be returned and the search will fail.

Answer: A

Explanation:

When you define a calculated field, you can specify the name of the field that the eval expression will create or modify. If the name of the calculated field matches the name of an existing extracted field, the calculated field will override the extracted field and replace its value with the result of the eval expression. This means that the original value of the extracted field will not be available for searching or analysis. To avoid this, you should use a unique name for your calculated field or use a different name for your extracted field²

1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, Configure calculated fields with props.conf.

NEW QUESTION 166

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 167

- (Exam Topic 2)

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

- A. sourcetype
- B. index
- C. source
- D. host

Answer: A

NEW QUESTION 170

- (Exam Topic 2)

When is a GET workflow action needed?

- A. To send field values to an external resource.
- B. To retrieve information from an external resource.
- C. To use field values to perform a secondary search.
- D. To define how events flow from forwarders to indexes.

Answer: B

NEW QUESTION 171

- (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 172

- (Exam Topic 2)

Tags can reference which of the following knowledge objects?

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

Answer: B

Explanation:

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

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

NEW QUESTION 174

- (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 179

- (Exam Topic 2)

What will you learn from the results of the following search? sourcetype=cisco_esa | transaction mid, dcid, icid | timechart avg(duration)

- A. The average time elapsed during each transaction for all transactions
- B. The average time for each event within each transaction
- C. The average time between each transaction

Answer: A

NEW QUESTION 184

- (Exam Topic 2) Consider the following search: Index=web sourcetype=access_combined

The log shows several events that share the same JSESSIONID value (SD404K289O2F151). View the events as a group. From the following list, which search groups events by JSESSIONID?

- A. index=web sourcetype=access_combined SD404K289O2F151 | table JSESSIONID
- B. index=web sourcetype=access_combined JSESSIONID <SD404K289O2F151>
- C. index=web sourcetype=access_combined | highlight JSESSIONID | search SD404K289O2F151
- D. index-web sourcetype=access_combined | transaction JSESSIONID | search SD404K289O2F151

Answer: B

NEW QUESTION 188

- (Exam Topic 2)

The stats command will create a _____ by default.

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

Answer: A

NEW QUESTION 193

- (Exam Topic 2)

Which knowledge object is used to normalize field names to comply with the Splunk Common Information Model (CIM)?

- A. Field alias
- B. Event types
- C. Search workflow action
- D. Tags

Answer: A

Explanation:

The correct answer is A. Field alias¹²³.

In Splunk, a field alias is a knowledge object that you can use to assign an alternate name to a field³. This can be particularly useful when you want to normalize your data to comply with the Splunk Common Information Model (CIM)¹².

The CIM provides a methodology for normalizing values to a common field name¹. It acts as a search-time schema to define relationships in the event data while leaving the raw machine data intact². By using field aliases, you can map vendor fields to common fields that are the same for each data source in a given domain⁴. This allows you to correlate events from different source types by normalizing these different occurrences to a common structure and naming convention¹.

NEW QUESTION 197

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 202

- (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 204

- (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 209

- (Exam Topic 2)

The macro weekly sales (2) contains the search string: index=games | eval ProductSales = \$Price\$ * \$AmountSold\$

Which of the following will return results?

- A. 'weekly sales (3)'
- B. 'weekly_sales(\$3.995, \$108)'
- C. 'weekly_sales (3.99, 10)'
- D. 'weekly sales (3.99, 10)'

Answer: C

Explanation:

To use a search macro in a search string, you need to place a back tick character (') before and after the macro name¹. You also need to use the same number of arguments as defined in the macro². The macro weekly sales (2) has two arguments: Price and AmountSold. Therefore, you need to provide two values for these arguments when you call the macro.

The option A is incorrect because it uses parentheses instead of back ticks around the macro name. The option B is incorrect because it uses underscores instead of spaces in the macro name. The option D is incorrect because it uses spaces instead of commas to separate the argument values.

Reference: 1 Use search macros in searches - Splunk Documentation 2 Define search macros in Settings - Splunk Documentation

NEW QUESTION 214

- (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 219

- (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 224

- (Exam Topic 2)

which of the following commands are used when creating visualizations(select all that apply.)

- A. Geom
- B. Choropleth
- C. Geostats
- D. iplocation

Answer: ACD

Explanation:

The following commands are used when creating visualizations: geom, geostats, and iplocation. Visualizations are graphical representations of data that show trends, patterns, or comparisons. Visualizations can have different types, such as charts, tables, maps, etc. Visualizations can be created by using various commands that transform the data into a suitable format for the visualization type. Some of the commands that are used when creating visualizations are:

➤ geom: This command is used to create choropleth maps that show geographic regions with different colors based on some metric. The geom command takes a KMZ file as an argument that defines the geographic regions and their boundaries. The geom command also takes a field name as an argument that specifies the metric to use for coloring the regions.

➤ geostats: This command is used to create cluster maps that show groups of events with different sizes and colors based on some metric. The geostats command takes a latitude and longitude field as arguments that specify the location of the events. The geostats command also takes a statistical function as an argument that specifies the metric to use for sizing and coloring the clusters.

➤ iplocation: This command is used to create location-based visualizations that show events with different attributes based on their IP addresses. The iplocation command takes an IP address field as an argument and adds some additional fields to the events, such as Country, City, Latitude, Longitude, etc. The iplocation command can be used with other commands such as geom or geostats to create maps based on IP addresses.

NEW QUESTION 225

- (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 228

- (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 232

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 236

- (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 239

- (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 243

- (Exam Topic 2)

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

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

Answer: D

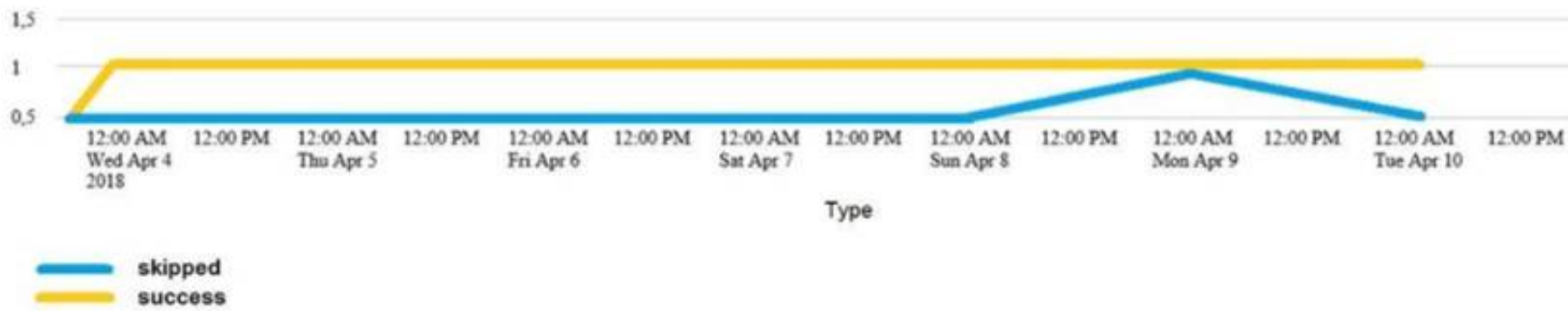
Explanation:

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

NEW QUESTION 246

- (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 251

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 256

- (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 259

- (Exam Topic 2)

What is the correct way to name a macro with two arguments?

- A. us_sales2
- B. us_sales(1,2)
- C. us_sale,2
- D. us_sales(2)

Answer: D

NEW QUESTION 264

- (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 268

- (Exam Topic 2)

If there are fields in the data with values that are " " or empty but not null, which of the following would add a value?

- A. | eval notNULL = if(isnull (notNULL), "0" notNULL)
- B. | eval notNULL = if(isnull (notNULL), "0"
- C. | eval notNULL = "" | nullfill value=0 notNULL
- D. | eval notNULL = "" fillnull value=0 notNULL

Answer: D

Explanation:

The correct answer is D. | eval notNULL = "" fillnull value=0 notNULL

- Option A is incorrect because it is missing a comma between the "0" and the notNULL in the if function. The correct syntax for the if function is if (condition, true_value, false_value).
- Option B is incorrect because it is missing the false_value argument in the if function. The correct syntax for the if function is if (condition, true_value, false_value).
- Option C is incorrect because it uses the nullfill command, which only replaces null values, not empty strings. The nullfill command is equivalent to fillnull value=null.
- Option D is correct because it uses the eval command to assign an empty string to the notNULL field, and then uses the fillnull command to replace the empty string with a zero. The fillnull command can replace any value with a specified replacement, not just null values.

NEW QUESTION 271

- (Exam Topic 2)

Where are the results of eval commands stored?

- A. In a field.
- B. In an index.
- C. In a KV Store.
- D. In a database.

Answer: A

Explanation:

<https://docs.splunk.com/Documentation/Splunk/8.0.2/SearchReference/Eval>

The eval command calculates an expression and puts the resulting value into a search results field.

- If the field name that you specify does not match a field in the output, a new field is added to the search results.
- If the field name that you specify matches a field name that already exists in the search results, the results of the eval expression overwrite the values in that field.

NEW QUESTION 275

- (Exam Topic 2)

For choropleth maps, splunk ships with the following KMZ files (select all that apply)

- A. States of the United States
- B. States and provinces of the united states and Canada
- C. Countries of the European Union
- D. Countries of the World

Answer: AD

Explanation:

Splunk ships with the following KMZ files for choropleth maps: States of the United States and Countries of the World. A KMZ file is a compressed file that contains a KML file and other resources. A KML file is an XML file that defines geographic features and their properties. A KMZ file can be used to create choropleth maps in Splunk by using the geom command. A choropleth map is a type of map that shows geographic regions with different colors based on some metric. Splunk ships with two KMZ files that define the geographic regions for choropleth maps:

- States of the United States: This KMZ file defines the 50 states of the United States and their boundaries. The name of this KMZ file is us_states.kmz and it is located in the \$SPLUNK_HOME/etc/apps/maps/appserver/static/geo directory.
 - Countries of the World: This KMZ file defines the countries of the world and their boundaries. The name of this KMZ file is world_countries.kmz and it is located in the \$SPLUNK_HOME/etc/apps/maps/appserver/static/geo directory.
- Splunk does not ship with KMZ files for States and provinces of the United States and Canada or Countries of the European Union. However, you can create your own KMZ files or download them from external sources and use them in Splunk.

NEW QUESTION 277

- (Exam Topic 2)

Which of the following describes the | transaction command?

- A. It is an SPL command that groups at least two events together based on shared values in selected fields.
- B. It allows an exchange of data from one Splunk index to another Splunk index.
- C. It is an SPL command that groups events together with shared values in selected fields.
- D. It allows an exchange of data from one Splunk system to another Splunk system.

Answer: C

Explanation:

- The transaction command is a Splunk command that finds transactions based on events that meet various constraints .
- Transactions are made up of the raw text (the _raw field) of each member, the time and date fields of the earliest member, as well as the union of all other fields of each member .
- The transaction command groups events together by matching one or more fields that have the same value across the events . For example, | transaction clientip will group events that have the same value the clientip field.

NEW QUESTION 279

- (Exam Topic 2)

How is a Search Workflow Action configured to run at the same time range as the original search?

- A. Set the earliest time to match the original search.
- B. Select the same time range from the time-range picker.
- C. Select the "Use the same time range as the search that created the field listing" checkbox.
- D. Select the "Overwrite time range with the original search" checkbox.

Answer: C

Explanation:

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

NEW QUESTION 283

- (Exam Topic 2)

Which of the following options will define the first event in a transaction?

- A. startswith
- B. with
- C. startingwith
- D. firstevent

Answer: A

Explanation:

The correct answer is A. startswith. The Explanation: is as follows:

- The transaction command is used to find transactions based on events that meet various constraints¹².
- Transactions are made up of the raw text (the _raw field) of each member, the time and date fields of the earliest member, as well as the union of all other fields of each member¹.
- The startswith option is used to define the first event in a transaction by specifying a search term or an expression that matches the event¹³.
- For example, | transaction clientip JSESSIONID startswith="view" will create transactions based on the clientip and JSESSIONID fields, and the first event in each transaction will contain the term “view” in the _raw field².

NEW QUESTION 288

.....

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](#)