

Exam Questions SPLK-1002

Splunk Core Certified Power User Exam

<https://www.2passeasy.com/dumps/SPLK-1002/>



NEW QUESTION 1

- (Exam Topic 1)

A space is an implied _____ in a search string.

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

Answer: B

Explanation:

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

NEW QUESTION 2

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 3

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 4

- (Exam Topic 1)

Which of the following actions can the eval command perform?

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

Answer: B

Explanation:

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

NEW QUESTION 5

- (Exam Topic 1)

In which of the following scenarios is an event type more effective than a saved search?

- A. When a search should always include the same time range.
- B. When a search needs to be added to other users' dashboards.
- C. When the search string needs to be used in future searches.
- D. When formatting needs to be included with the search string.

Answer:

C

Explanation:Reference: <https://answers.splunk.com/answers/4993/eventtype-vs-saved-search.html>

An event type is a way to categorize events based on a search string that matches the events². You can use event types to simplify your searches by replacing long or complex search strings with short and simple event type names². An event type is more effective than a saved search when the search string needs to be used in future searches because it allows you to reuse the search string without having to remember or type it again². Therefore, option C is correct, while options A, B and D are incorrect because they are not scenarios where an event type is more effective than a saved search.

NEW QUESTION 6

- (Exam Topic 1)

Which of the following searches show a valid use of macro? (Select 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:**

Reference:

<https://answers.splunk.com/answers/574643/field-showing-an-additional-and-not-visible-value-1.html>

To use a macro in a search, you must enclose the macro name and any arguments in single quotation marks¹. For example, 'my_macro(arg1,arg2)' is a valid way to use a macro with two arguments. You can use macro anywhere in your search string where you would normally use a search command or expression¹. Therefore, options A and C are valid searches that use macros, while options B and D are invalid because they do not enclose the macros in single quotation marks.

NEW QUESTION 7

- (Exam Topic 1)

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

- A. Use the scats 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 8

- (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 9

- (Exam Topic 1)

Which of the following statements describe GET workflow actions?

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

Answer: D**Explanation:**

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

NEW QUESTION 10

- (Exam Topic 1)

Which of the following statements describes POST workflow actions?

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

Answer: D

Explanation:

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

NEW QUESTION 10

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 15

- (Exam Topic 1)

How does a user display a chart in stack mode?

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

Answer: C

Explanation:

A chart is a graphical representation of your search results that shows the relationship between two or more fields². You can display a chart in stack mode by changing the Stack Mode option in the Format menu². Sta mode allows you to stack multiple series on top of each other in a chart to show the cumulative values of each series². Therefore, option C is correct, while options A, B and D are incorrect because they are not ways to display a chart in stack mode.

NEW QUESTION 17

- (Exam Topic 1)

A calculated field maybe based on which of the following?

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

Answer: B

Explanation:

As mentioned before, a calculated field is a field that you create based on the value of another field or fields². A calculated field can be based on extracted fields, which are fields that are extracted from your raw data using various methods such as regular expressions, delimiters or key-value pairs². Therefore, option B is correct, while options A, C and D are incorrect because they are not types of fields that a calculated field can be based on.

NEW QUESTION 18

- (Exam Topic 1)

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

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

Answer: ABC

Explanation:

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

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

NEW QUESTION 20

- (Exam Topic 1)

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

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

Answer: BCD

Explanation:

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

NEW QUESTION 24

- (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 29

- (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 31

- (Exam Topic 1)

Which are valid ways to create an event type? (select all that apply)

- A. By using the `searchtypes` command in the search bar.
- B. By editing the `event_type` stanza in the `props.conf` file.
- C. By going to the Settings menu and clicking Event Types > New.
- D. By selecting an event in search results and clicking Event Actions > Build Event Type.

Answer: CD

Explanation:

Event types are custom categories of events that are based on search criteria. Event types can be used to label events with meaningful names, such as error, success, login, logout, etc. Event types can also be used to create transactions, alerts, reports, dashboards, etc. Event types can be created in two ways:

- By going to the Settings menu and clicking Event Types > New. This will open a form where you can enter the name, description, search string, app context, and tags for the event type.
 - By selecting an event in search results and clicking Event Actions > Build Event Type. This will open a dialog box where you can enter the name and description for the event type. The search string will be automatically populated based on the selected event.
- Event types cannot be created by using the searchtypes command in the search bar, as this command does not exist in Splunk. Event types can also be created by editing the event_type stanza in the transforms.conf file, not the props.conf file.

NEW QUESTION 33

- (Exam Topic 1)

What is the correct syntax to search for a tag associated with a value on a specific fields?

- A. Tag-<field?
- B. Tag<filed(tagname.)
- C. Tag=<filed>::<tagname>
- D. Tag::<filed>=<tagname>

Answer: D

Explanation:

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

A tag is a descriptive label that you can apply to one or more fields or field values in your events². You can use tags to simplify your searches by replacing long or complex field names or values with short and simple tags². To search for a tag associated with a value on a specific field, you can use the following syntax: tag::<field>=<tagname>². For example, tag::status=error will search for events where the status field has a tag named error. Therefore, option D is correct, while options A, B and C are incorrect because they do not follow the correct syntax for searching tags.

NEW QUESTION 36

- (Exam Topic 1)

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

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

Answer: ABCD

Explanation:

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

NEW QUESTION 39

- (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 44

- (Exam Topic 1)

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

- A. CSV

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

Answer: A

Explanation:

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

NEW QUESTION 45

- (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 50

- (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 53

- (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 54

- (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 57

- (Exam Topic 2)

The timechart command is an example of which of the following command types?

- A. Orchestrating
- B. Transforming
- C. Statistical
- D. Generating

Answer: B

Explanation:

The correct answer is B. Transforming. The explanation is as follows:

- The timechart command is a Splunk command that creates a time series chart with corresponding table of statistics¹².
- A timechart is a statistical aggregation applied to a field to produce a chart, with time used as the X-axis¹. You can specify a split-by field, where each distinct value of the split-by field becomes a series in the chart¹.
- Transforming commands are commands that change the format of the search results into a data structure that can be easily visualized³. Transforming commands often use stats functions to aggregate and summarize data³.
- Therefore, the timechart command is an example of a transforming command, as it transforms the search results into a chart and a table using stats functions¹²³.

NEW QUESTION 59

- (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 62

- (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 64

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 67

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 69

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

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

The syntax for the where command is:

| where <expression>

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

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

B, you can use the following syntax:

| where A=B

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

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

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

References:

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

NEW QUESTION 72

- (Exam Topic 2)

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

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

Answer: BCD

Explanation:

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

NEW QUESTION 76

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

specified fields in your search results with tags¹.

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

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

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

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

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

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

NEW QUESTION 78

- (Exam Topic 2)

A calculated field is a shortcut for performing repetitive, long, or complex transformations using which of the following commands?

- A. transaction
- B. lookup
- C. stats
- D. eval

Answer: D

Explanation:

The correct answer is D. `eval`.

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 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.

A calculated field is a shortcut for performing repetitive, long, or complex transformations using the `eval` command. The `eval` command is used to create or modify fields by using expressions. The `eval` command can perform mathematical, string, date and time, comparison, logical, and other operations on fields or values².

For example, if you want to create a new field named `total` that is the sum of two fields named `price` and `tax`, you can use the `eval` command as follows:

```
| eval total=price+tax
```

However, if you want to use this new field in multiple searches, reports, or dashboards, you can create a calculated field instead of writing the `eval` command every time. To create a calculated field with Splunk Web, you need to go to Settings > Fields > Calculated Fields and enter the name of the new field (`total`), the name of the sourcetype (`sales`), and the `eval` expression (`price+tax`). This will create a calculated field named `total` that will be added to all events with the sourcetype `sales` at search time. You can then use the `total` field like any other extracted field without writing the `eval` expression¹.

The other options are not correct because they are not related to calculated fields. These options are:

- A. `transaction`: This command is used to group events that share some common values into a single record, called a transaction. A transaction can span multiple events and multiple sources, and can be useful for correlating events that are related but not contiguous³.
- B. `lookup`: This command is used to enrich events with additional fields from an external source, such as a CSV file or a database. A lookup can add fields to events based on the values of existing fields, such as `host`, `source`, `sourcetype`, or any other extracted field.
- C. `stats`: This command is used to calculate 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 fields.

References:

- [About calculated fields](#)
- [eval command overview](#)
- [transaction command overview](#)
- [\[lookup command overview\]](#)
- [\[stats command overview\]](#)

NEW QUESTION 82

- (Exam Topic 2)

In most large Splunk environments, what is the most efficient command that can be used to group events by fields/

- A. join
- B. stats
- C. streamstats
- D. transaction

Answer: B

Explanation:

<https://docs.splunk.com/Documentation/Splunk/8.0.2/Search/Abouttransactions>

In other cases, it's usually better to use the `stats` command, which performs more efficiently, especially in a distributed environment. Often there is a unique ID in the events and `stats` can be used.

NEW QUESTION 83

- (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 85

- (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 86

- (Exam Topic 2)

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

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

Answer: D

Explanation:

The correct answer is D.

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

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

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

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

```
my_macro(web)
```

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

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

References:

> Use search macros in searches

NEW QUESTION 88

- (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 89

- (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 92

- (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 96

- (Exam Topic 2)

This clause is used to group the output of a stats command by a specific name.

- A. Rex
- B. As
- C. List
- D. By

Answer: B

NEW QUESTION 101

- (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 103

- (Exam Topic 2)

The macro weekly_sales (2) contains the search string:

index—games | eval Product Sales = \$price\$ \$Amount\$ | sort Product Sales desc 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 104

- (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 109

- (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 112

- (Exam Topic 2)

What is the Splunk Common Information Model (CIM)?

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

Answer: B

Explanation:

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

NEW QUESTION 115

- (Exam Topic 2)

In the Field Extractor Utility, this button will display events that do not contain extracted fields. Select your answer.

- A. Selected-Fields
- B. Non-Matches
- C. Non-Extractions
- D. Matches

Answer: B

Explanation:

The Field Extractor Utility (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 has a button that displays events that do not contain extracted fields, which is the Non-Matches button². The Non-Matches button shows you the events that do not match the regular expression that you have defined for your field extraction². This way, you can check if your field extraction is accurate and complete². Therefore, option B is correct, while options A, C and D are incorrect because they are not buttons that display events that do not contain extracted fields.

NEW QUESTION 120

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 125

- (Exam Topic 2)

Which statement is true?

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

Answer: C

Explanation:

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

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

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

NEW QUESTION 128

- (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 129

- (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 134

- (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 139

- (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 140

- (Exam Topic 2)

These allow you to categorize events based on search terms. Select your answer.

- A. Groups
- B. Event Types
- C. Macros
- D. Tags

Answer: B

NEW QUESTION 144

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 149

- (Exam Topic 2)

A report scheduled to run every 15 mins. but takes 17 mins. to complete is in danger of being _____.

- A. skipped or deferred
- B. automatically accelerated
- C. deleted
- D. all of the above

Answer: A

Explanation:

A report that is scheduled to run every 15 minutes but takes 17 minutes to complete is in danger of being skipped or deferred². This means that Splunk may skip some scheduled runs of the report if they overlap with previous runs that are still in progress or defer them until the previous runs are finished². This can affect the accuracy and timeliness of the report results and notifications². Therefore, option A is correct, while options B, C and D are incorrect because they are not consequences of a report taking longer than its schedule interval.

NEW QUESTION 152

- (Exam Topic 2)

Select this in the fields sidebar to automatically pipe you search results to the rare command

- A. events with this field
- B. rare values
- C. top values by time
- D. top values

Answer: B

Explanation:

The fields sidebar is a panel that shows the fields that are present in your search results². The fields sidebar has two sections: selected fields and interesting fields². 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.

Interesting field are fields that appear in at least 20 percent of events or have high variability among values². For each field in the fields sidebar, you can select one of the following options: events with this field, rare values, top values by time or top values². If you select rare values, Splunk will automatically pipe your search results to the rare command, which shows the least common values of a field². Therefore, option B is correct, while options A, C and D are incorrect because they do not pipe your search results to the rare command.

NEW QUESTION 157

- (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 159

- (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 163

- (Exam Topic 2)

If a search returns _____ it can be viewed as a chart.

- A. timestamps
- B. statistics
- C. events
- D. keywords

Answer: B

Explanation:

If a search returns statistics, it can be viewed as a chart². Statistics are tabular data that show the relationship between two or more fields². You can create statistics by using commands such as stats, chart or timechart². You can view statistics as a chart by selecting the Visualization tab in the Search app and choosing a chart type such as column, line or pie². Therefore, option B is correct, while options A, C and D are incorrect because they are not types of data that can be viewed as a chart.

NEW QUESTION 167

- (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 172

- (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 175

- (Exam Topic 2)

Which of the following eval command functions is valid?

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

Answer: D

Explanation:

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

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

NEW QUESTION 179

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 183

- (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 184

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 189

- (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 192

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 193

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 197

- (Exam Topic 2)

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

| eval productINFO=coalesce(productName,productid)

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

Answer: B

Explanation:

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

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

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

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

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

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

| eval ip=coalesce(clientip,ipaddress)

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

| eval productINFO=coalesce(productName,productid)

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

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

References:

- Search Command> Coalesce
- USAGE OF SPLUNK EVAL FUNCTION : COALESCE

NEW QUESTION 200

- (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 204

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 206

- (Exam Topic 2)

Which is not a comparison operator in Splunk

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

Answer: E

Explanation:

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

NEW QUESTION 208

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 209

- (Exam Topic 2)

When extracting fields, we may choose to use our own regular expressions

- A. True
- B. False

Answer: A

NEW QUESTION 210

- (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 212

- (Exam Topic 2)

Which of the following is NOT a stats function:

- A. sum
- B. addtotals
- C. count
- D. avg

Answer: B

Explanation:

The stats command is used to calculate summary statistics for your search results such as count, sum, avg, min, max and more². The stats command supports various functions that you can use to perform calculations on your fields². However, addtotals is not a stats function but a separate command that adds a row or column with the total of the values in each group². Therefore, option B is correct, while options A, C and D are incorrect because they are valid stats functions.

NEW QUESTION 216

- (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 219

- (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 222

- (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 223

- (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 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 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 234

- (Exam Topic 2)

Which search retrieves events with the event type web_errors?

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

Answer: B

Explanation:

The correct answer is B. eventtype=web_errors.

An event type is a way to categorize events based on a search. An event type assigns a label to events that match a specific search criteria. Event types can be used to filter and group events, create alerts, or generate reports¹.

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

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

eventtype=web_errors

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

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

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

References:

- About event types
- About tags
- Search command cheatsheet

NEW QUESTION 238

- (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 240

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 245

- (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 248

- (Exam Topic 2)

What is the correct format for naming a macro with multiple arguments?

- A. monthly_sales(argument 1, argument 2, argument 3)
- B. monthly_sales(3)
- C. monthly_sales[3]
- D. monthly_sales[argument 1, argument 2, argument 3]

Answer: C

Explanation:

The correct format for naming a macro with multiple arguments is monthly_sales3. The square brackets indicate that the macro has arguments, and the number indicates how many arguments it has. The arguments are separated by commas when calling the macro, such as monthly_sales[region,salesperson,date].

NEW QUESTION 251

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 256

- (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 258

- (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 263

- (Exam Topic 2)

The time range specified for a historical search defines the _____.-----questionable on ans

- A. Amount of data shown on the timeline as data streams in
- B. Amount of data fetched from index matching that time range
- C. Time range for the static results

Answer: B

Explanation:

The time range specified for a historical search defines the amount of data fetched from the index matching that time range². A historical search is a search that runs over a fixed period of time in the past². When you run a historical search, Splunk searches the index for events that match your search string and fall within the specified time range². Therefore, option B is correct, while options A and C are incorrect because they are not what the time range defines for a historical search.

NEW QUESTION 265

- (Exam Topic 2)

Which of the following statements would help a user choose between the transaction and stats commands?

- A. state can only group events using IP addresses.
- B. The transaction command is faster and more efficient.
- C. There is a 1000 event limitation with the transaction command.
- D. Use state when the events need to be viewed as a single event.

Answer: C

Explanation:

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

One of the statements that would help a user choose between the transaction and stats commands is that there is a 1000 event limitation with the transaction command³. The transaction command is used to group events that share a common value for one or more fields into transactions³. The transaction command has a default limit of 1000 events per transaction, which means that it will not group more than 1000 events into a single transaction³. This limit can be changed by using the maxevents parameter, but it can affect the performance and memory usage of Splunk³. Therefore, option C is correct, while options A, B and D are incorrect because they are not statements that would help a user choose between the transaction and stats commands.

NEW QUESTION 269

- (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 271

- (Exam Topic 2)

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

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

Answer: AB

Explanation:

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

NEW QUESTION 276

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-1002 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-1002 Product From:

<https://www.2passeasy.com/dumps/SPLK-1002/>

Money Back Guarantee

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