

Splunk

Exam Questions SPLK-1002

Splunk Core Certified Power User Exam



NEW QUESTION 1

- (Exam Topic 1)

A space is an implied _____ in a search string.

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

Answer: B

Explanation:

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

NEW QUESTION 2

- (Exam Topic 1)

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)

When should you use the transaction command instead of the stats command?

- A. When you need to group on multiple values.
- B. When duration is irrelevant in search result
- C. .
- D. When you have over 1000 events in a transaction.
- E. When you need to group based on start and end constraints.

Answer: D

Explanation:

The transaction command is used to group events into transactions based on some common characteristics, such as fields, time, or both. The transaction command can also specify start and end constraints for the transactions, such as a field value that indicates the beginning or the end of a transaction. The stats command is used to calculate summary statistics on the events, such as count, sum, average, etc. The stats command cannot group events based on start and end constraints, but only on fields or time buckets. Therefore, the transaction command should be used instead of the stats command when you need to group events based on start and end constraints.

NEW QUESTION 4

- (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 events. You can use event types to simplify your searches by replacing long or complex search strings with short and simple event type names. 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 again. 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 5

- (Exam Topic 1)

Which of the following statements about tags is true?

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

Answer: C

Explanation:

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

NEW QUESTION 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)

What do events in a transaction have In common?

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

Answer: D

Explanation:

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

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

NEW QUESTION 9

- (Exam Topic 1)

The Field Extractor (FX) is used to extract a custom field. A report can be created using this custom field. The created report can then be shared with other people in the organization. If another person in the organization runs the shared report and no results are returned, why might this be? (select all that apply)

- A. Fast mode is enabled.
- B. The dashboard is private.
- C. The extraction is private
- D. The person in the organization running the report does not have access to the index.

Answer: CD

Explanation:

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

NEW QUESTION 10

- (Exam Topic 1)

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

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

Answer: ABD

Explanation:

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

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

NEW QUESTION 10

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 12

- (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 13

- (Exam Topic 1)

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

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

Answer: BCD

Explanation:

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

- > It filters the events by the sourcetype `access_combined`, which is a predefined sourcetype for Apache web server logs.
- > It groups the events by the field `JSESSIONID`, which is a unique identifier for each user session.

➤ It creates a single event from each group of events that share the same JSESSIONID value. This single event will have some additional fields created by the transaction command, such as duration, eventcount, and starttime. Therefore, the statements B, C, and D are true.

NEW QUESTION 17

- (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 19

- (Exam Topic 1)

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

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

Answer: B

Explanation:

The transaction command is used to group events that share a common value for one or more fields into transactions². The transaction command assigns a transaction ID to each group of events and creates new fields such as duration, eventcount and eventlist for each transaction². To identify all of the contributing events within a transaction that contains at least one REJECT event, you can use the following syntax: index=main | transaction sessionid | search REJECT². This search will first group the events by sessionid, then filter out the transactions that do not contain REJECT in any of their events². Therefore, option B is correct, while options A, C and D are incorrect because they do not follow the correct syntax for using the transaction command or the search command.

NEW QUESTION 24

- (Exam Topic 1)

Which of the following statements describe the Common Information Model (CIM)? (select all that apply)

- A. CIM is a methodology for normalizing data.
- B. CIM can correlate data from different sources.
- C. The Knowledge Manager uses the CIM to create knowledge objects.
- D. CIM is an app that can coexist with other apps on a single Splunk deployment.

Answer: ABC

Explanation:

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

The Common Information Model (CIM) is a methodology for normalizing data from different sources and making it easier to analyze and report on it³. The CIM defines a common set of fields and tags for various domains such as Alerts, Email, Database, Network Traffic, Web and more³. One of the statements that describe the CIM is that it is a methodology for normalizing data, which means that it provides a standard way to name and structure data from different sources so that they can be compared and correlated³. Therefore, option A is correct. Another statement that describes the CIM is that it can correlate data from different sources, which means that it enables you to run searches and reports across data from different sources that share common fields and tags³. Therefore, option B is correct. Another statement that describes the CIM is that the Knowledge Manager uses the CIM to create knowledge objects, which means that the person who is responsible for creating and managing knowledge objects such as data models, field aliases, tags and event types can use the CIM as a guide to make their knowledge objects consistent and compatible with other apps and add-ons³. Therefore, option C is correct. Option D is incorrect because it does not describe the CIM but rather one of its components.

NEW QUESTION 26

- (Exam Topic 1)

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

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

Answer: B

Explanation:

The Splunk Common Information Model (CIM) add-on helps you normalize your data from different sources and make it easier to analyze and report on it³. One of

the functionalities that the CIM add-on relies on to normalize fields with different names is field aliases³. Field aliases allow you to assign an alternative name to an existing field without changing the original field name or value². By using field aliases, you can map different field names from different sources or sourcetypes to a common field name that conforms to the CIM standard³. Therefore, option B is correct, while options A, C and D are incorrect.

NEW QUESTION 31

- (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 35

- (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 36

- (Exam Topic 1)

What does the transaction command do?

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

Answer: B

Explanation:

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

NEW QUESTION 41

- (Exam Topic 1)

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

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

Answer: BCD

Explanation:

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

The Field Extractor (FX) is a tool that helps you extract fields from your data using delimiters or regular expressions. Delimiters are characters or strings that separate fields in your data. The FX can detect some common delimiters automatically, such as pipes (|), spaces (), commas (,), semicolons (;), etc. The FX

cannot detect tabs (t) as delimiters automatically, but you can specify them manually in the FX interface.

NEW QUESTION 42

- (Exam Topic 1)

Which of the following eval command function is valid?

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

Answer: D

Explanation:

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

NEW QUESTION 45

- (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 48

- (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 53

- (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 55

- (Exam Topic 2)

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

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

D. #

Answer: B

Explanation:

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

NEW QUESTION 60

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 63

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 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 200. 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 72

- (Exam Topic 2)

By default, how is acceleration configured in the Splunk Common Information Model (CIM) add-on?

- A. Turned off
- B. Turned on
- C. Determined automatically based on the sourcetype.
- D. Determined automatically based on the data source.

Answer: D

Explanation:

By default, acceleration is determined automatically based on the data source in the Splunk Common Information Model (CIM) add-on. The Splunk CIM Add-on is an app that provides common data models for various domains, such as network traffic, web activity, authentication, etc. The CIM Add-on allows you to normalize and enrich your data using predefined fields and tags. The CIM Add-on also allows you to accelerate your data models for faster searches and reports. Acceleration is a feature that pre-computes summary data for your data models and stores them in tsidx files. Acceleration can improve the performance and

efficiency of your searches and reports that use data models.

By default, acceleration is determined automatically based on the data source in the CIM Add-on. This means that Splunk will decide whether to enable or disable acceleration for each data model based on some factors, such as data volume, data type, data model complexity, etc. However, you can also manually enable or disable acceleration for each data model by using the Settings menu or by editing the `datamodels.conf` file.

NEW QUESTION 74

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 79

- (Exam Topic 2)

Field aliases are used to _____ data

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

Answer: D

NEW QUESTION 82

- (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 83

- (Exam Topic 2)

What fields does the `transaction` command add to the raw events? (select all that apply)

- A. count
- B. duration
- C. eventcount
- D. transaction id

Answer: BD

Explanation:

Hello, this is Bing. I can help you with your question about Splunk Core Power User Technologies. The correct answers are B. duration and D. transaction id. The explanation is as follows:

- The transaction command is a Splunk command that finds transactions based on events that meet various constraints¹².
- Transactions are made up of the raw text (the `_raw` field) of each member, the time and date fields of the earliest member, as well as the union of all other fields of each member¹².
- The transaction command adds some fields to the raw events that are part of the transaction¹²³. These fields are:
 - duration: The difference, in seconds, between the timestamps for the first and last events in the transaction¹²³.
 - eventcount: The number of events in the transaction¹²³.
 - transaction_id: A unique identifier for each transaction³. This field is useful for filtering or joining transactions³.
- Therefore, the fields that the transaction command adds to the raw events are duration and transaction_id, which are options B and D in your question.

NEW QUESTION 86

- (Exam Topic 2)

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

- A. Using the span argument.
- B. Using the duration argument.
- C. Using the interval argument.
- D. Adjusting the fieldformat options.

Answer: A

NEW QUESTION 90

- (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 95

- (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 97

- (Exam Topic 2)

A user runs the following search:

`index=X sourcetype=Y | chart count (domain) as count, sum (price) as sum by product, action usenull=f useother=f`
 Which of the following table headers match the order this command creates?

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

Answer: C

Explanation:

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

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

In the given search, the chart command is used with two functions (count and sum), two fields (domain and price), and two fields to group by (product and action). The usenull=f and useother=f options are used to exclude null values and other values from the chart².

The chart command creates a table with headers that match the order of the fields and functions in the command¹. The headers for the count function are prefixed with count:, and the headers for the sum function are prefixed with sum:¹. The values of the product and action fields are used as the suffixes for the headers¹. Therefore, the table headers created by this command are Product, count: addtocart, count: remove, count: purchase, sum: addtocart, sum: remove, and sum: purchase¹.

NEW QUESTION 99

- (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 101

- (Exam Topic 2)

The macro weekly_sales (2) contains the search string:

index—games | eval Product Sales = \$price\$ \$Amount\$ | d\$ 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 105

- (Exam Topic 2)

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

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

Answer: ABC

Explanation:

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

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

NEW QUESTION 110

- (Exam Topic 2)

How are event types different from saved reports?

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

Answer: D

Explanation:

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

The explanation is as follows:

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

NEW QUESTION 112

- (Exam Topic 2)

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

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

Answer: ABD

Explanation:

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

NEW QUESTION 117

- (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 122

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 123

- (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 128

- (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 131

- (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 136

- (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 138

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

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

The delimiters method is designed for structured event data: data from files with headers, where all of the fields in the events are separated by a common delimiter, such as a comma or space¹. You select a sample event, identify the delimiter, and then rename the fields that the field extractor finds¹. This method is simpler and faster than the regular expression method, but it may not work well with complex or irregular data formats¹.

Reference:

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

NEW QUESTION 140

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

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

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

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

- > About calculated fields
- > About lookups
- > Search time processing

NEW QUESTION 143

- (Exam Topic 2)

Which of the following statements best describes a macro?

- A. A macro is a method of categorizing events based on a search.
- B. A macro is a way to associate an additional (new) name with an existing field name.
- C. A macro is a portion of a search that can be reused in multiple place

D. A macro is a knowledge object that enables you to schedule searches for specific events.

Answer: C

Explanation:

The correct answer is C. A macro is a portion of a search that can be reused in multiple places.

A macro is a way to reuse a piece of SPL code in different searches. A macro can be any part of a search, such as an eval statement or a search term, and does not need to be a complete command. A macro can also take arguments, which are variables that can be replaced by different values when the macro is called. A macro can also contain another macro within it, which is called a nested macro¹.

To create a macro, you need to define its name, definition, arguments, and description in the Settings > Advanced Search > Search Macros page in Splunk Web or in the macros.conf file. To use a macro in a search, you need to enclose the macro name in backtick characters (`) and provide values for the arguments if any¹.

For example, if you have a macro named my_macro that takes one argument named object and has the following definition:

```
search sourcetype= object
```

You can use it in a search by writing: my_macro(web)

This will expand the macro and run the following SPL code: search sourcetype=web

The benefits of using macros are that they can simplify complex searches, reduce errors, improve readability, and promote consistency¹.

The other options are not correct because they describe other types of knowledge objects in Splunk, not macros. These objects are:

- > A. An event type is a method of categorizing events based on a search. An event type assigns a label to events that match a specific search criteria. Event types can be used to filter and group events, create alerts, or generate reports².
- > B. A field alias is a way to associate an additional (new) name with an existing field name. A field alias can be used to normalize fields from different sources that have different names but represent the same data. Field aliases can also be used to rename fields for clarity or convenience³.
- > D. An alert is a knowledge object that enables you to schedule searches for specific events and trigger actions when certain conditions are met. An alert can be used to monitor your data for anomalies, errors, or other patterns of interest and notify you or others when they occur⁴.

References:

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

NEW QUESTION 147

- (Exam Topic 2)

When defining a macro, what are the required elements?

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

Answer: C

Explanation:

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

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

NEW QUESTION 148

- (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 152

- (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 156

- (Exam Topic 2)
 How is a macro referenced in a search?

- A. By using the macroname command.
- B. By using the macro command.
- C. By enclosing the macro name in backtick characters (`).
- D. By enclosing the macro name in single-quote characters (').

Answer: C

Explanation:

The correct answer is C. By enclosing the macro name in backtick characters (`).
 A macro is a way to reuse a piece of SPL code in different searches. A macro can take arguments, which are variables that can be replaced by different values when the macro is called. A macro can also contain another macro within it, which is called a nested macro.
 To reference a macro in a search, you need to enclose the macro name in backtick characters (`). For example, if you have a macro named my_macro` that takes one argument, you can reference it in a search by using the following syntax:

```
| my_macro(argument) | ...
```

This will replace the macro name and argument with the SPL code contained in the macro definition. For example, if the macro definition is:

```
[my_macro(argument)] search sourcetype=$argument$ And you reference it in a search with:
```

```
index=main | my_macro(web) | stats count by host
```

This will expand the macro and run the following SPL code: index=main | search sourcetype=web | stats count by host

References:
 > Use search macros in searches

NEW QUESTION 159

- (Exam Topic 2)
 The gauge command:

- A. creates a single-value visualization
- B. allows you to set colored ranges for a single-value visualization
- C. creates a radial gauge visualization

Answer: B

NEW QUESTION 161

- (Exam Topic 2)
 The fields sidebar does not show _____. (Select all that apply.)

- A. interesting fields
- B. selected fields
- C. all extracted fields

Answer: C

Explanation:

The fields sidebar is a panel that shows the fields that are present in your search results. The fields sidebar does not show all extracted fields, which are fields that are extracted from your raw data using various methods such as regular expressions, delimiters or key-value pairs. The fields sidebar only shows selected fields and interesting fields. 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 command. Interesting fields are fields that appear in at least 20 percent of events or have high variability among values. Therefore, option C is correct, while options A and B are incorrect because they are types of fields that the fields sidebar does show.

NEW QUESTION 164

- (Exam Topic 2)
 This function of the stats command allows you to identify the number of values a field has.

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

Answer: D

NEW QUESTION 168

- (Exam Topic 2) Consider the following search: Index=web sourcetype=access_combined
 The log shows several events that share the same JSESSIONID value (SD404K289O2F151). View the events as a group. From the following list, which search groups events by JSESSIONID?

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

Answer: B

NEW QUESTION 173

- (Exam Topic 2)
 Which of the following statements about tags is true?

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

Answer: B

Explanation:

- Tags are a knowledge object that allow you to assign an alias to one or more field values . Tags are applied to events at search time and can be used as search terms or filters .
- Tags can help you make your data more understandable by replacing cryptic or complex field values with meaningful names . For example, you can tag the value 200 in the status field as success, or value 404 as not_found .

NEW QUESTION 178

- (Exam Topic 2)

The timechart command buckets data in time intervals depending on:

- A. the number of events returned
- B. the selected time range
- C. the type of visualization selected

Answer: B

Explanation:

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

NEW QUESTION 180

- (Exam Topic 2)

The stats command will create a _____ by default.

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

Answer: A

NEW QUESTION 181

- (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 183

- (Exam Topic 2)

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

- A. chart, timechart, stats, eventstats
- B. chart, timechart, stats, diff
- C. chart, timeehart, datamodel, pivot
- D. chart, timecha:t, stats, pivot

Answer: A

Explanation:

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

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

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

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

- chart: This command creates a table or a chart that shows the relationship between two or more fields. It can be used to aggregate values, count occurrences, or calculate statistics³.
- timechart: This command creates a table or a chart that shows how a field changes over time. It can be used to plot trends, patterns, or outliers⁴.
- stats: This command calculates summary statistics on the fields in the search results, such as count, sum, average, etc. It can be used to group and aggregate data by one or more fields⁵.
- eventstats: This command calculates summary statistics on the fields in the search results, similar to stats, but it also adds the results to each event as new fields. It can be used to compare events with the overall statistics.

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

- | chart count by user : This command creates a table or a chart that shows how many transactions each user has.
- | timechart span=1h avg(duration) by user : This command creates a table or a chart that shows the average duration of transactions for each user per hour.
- | stats sum(eventcount) as total_events by user : This command creates a table that shows the total number of events for each user across all transactions.
- | eventstats avg(duration) as avg_duration : This command adds a new field named avg_duration to each transaction that shows the average duration of all transactions.

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

- diff: This command compares two search results and shows the differences between them. It is not a transforming command and it does not work with transactions.
- datamodel: This command retrieves data from a data model, which is a way to organize and categorize data in Splunk. It is not a transforming command and it does not work with transactions.
- pivot: This command creates a pivot report, which is a way to analyze data from a data model using a graphical interface. It is not a transforming command and it does not work with transactions.

References:

- About transforming commands
- About transactions
- chart command overview
- timechart command overview
- stats command overview
- [eventstats command overview]
- [diff command overview]
- [datamodel command overview]
- [pivot command overview]

NEW QUESTION 184

- (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 185

- (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 190

- (Exam Topic 2)

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

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

Answer: ACD

Explanation:

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

- geom: This command is used to create choropleth maps that show geographic regions with different colors based on some metric. The geom command takes a KMZ file as an argument that defines the geographic regions and their boundaries. The geom command also takes a field name as an argument that specifies the metric to use for coloring the regions.
- geostats: This command is used to create cluster maps that show groups of events with different sizes and colors based on some metric. The geostats command takes a latitude and longitude field as arguments that specify the location of the events. The geostats command also takes a statistical function as an argument that specifies the metric to use for sizing and coloring the clusters.
- iplocation: This command is used to create location-based visualizations that show events with different attributes based on their IP addresses. The iplocation command takes an IP address field as an argument and adds some additional fields to the events, such as Country, City, Latitude, Longitude, etc. The iplocation command can be used with other commands such as geom or geostats to create maps based on IP addresses.

NEW QUESTION 192

- (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 195

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 199

- (Exam Topic 2)

Calculated fields can be based on which of the following?

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

Answer: B

Explanation:

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

NEW QUESTION 203

- (Exam Topic 2)

Which of the following statements describes an event type?

- A. A log level measurement: info, warn, error.
- B. A knowledge object that is applied before fields are extracted.
- C. A field for categorizing events based on a search string.
- D. Either a log, a metric, or a trace.

Answer: C

Explanation:

This is because an event type is a knowledge object that assigns a user-defined name to a set of events that match a specific search criteria. For example, you can create an event type named successful_purchase for events that have sourcetype=access_combined, status=200, and action=purchase. Then, you can use eventtype=successful_purchase as a search term to find those events. You can also use event types to create alerts, reports, and dashboards. You can learn more about event types from the Splunk documentation¹. The other options are incorrect because they do not describe what an event type is. A log level measurement is a field that indicates the severity of an event, such as info, warn, or error. A knowledge object that is applied before fields are extracted is a source type, which identifies the format and structure of the data. Either a log, a metric, or a trace is a type of data that Splunk can ingest and analyze, but not an event type.

NEW QUESTION 208

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

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

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

`outer_macro (argument1, inner_macro (argument2))`

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

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

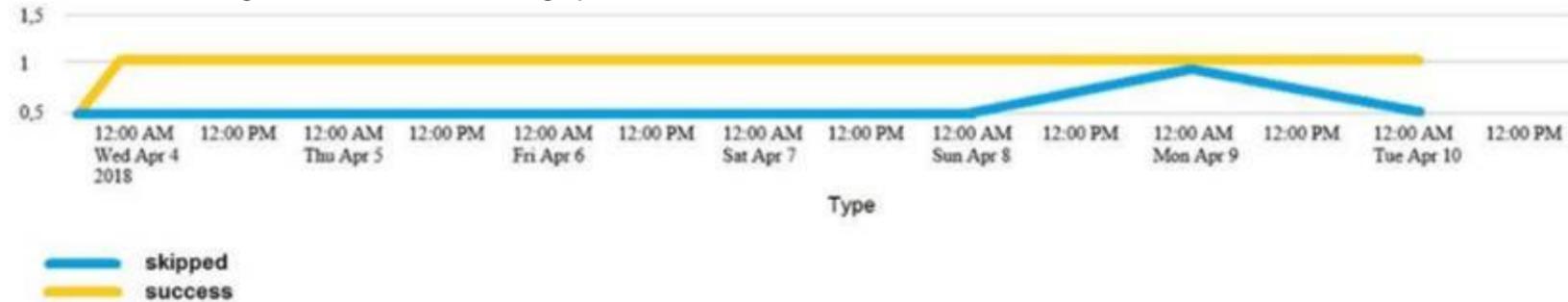
This will expand the macros with the corresponding arguments and run the SPL code contained in them. References:

- > Search macro examples
- > Use search macros in searches

NEW QUESTION 210

- (Exam Topic 2)

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



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

Answer: C

Explanation:

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

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

The search does the following:

- > It uses `index_internal` to specify the internal index that contains Splunk logs and metrics.
 - > It uses `sourcetype=Savesplunker` to filter events by the sourcetype that indicates the Splunk Enterprise Security app.
 - > It uses `fields sourcetype, status` to keep only the sourcetype and status fields in the events.
 - > It uses `transaction status maxspan=1d` to group events into transactions based on the status field with a maximum time span of one day between the first and last events in a transaction.
 - > It uses `timechart count by status` to create a time-based chart that shows the count of transactions for each status value over time.
- The graph shows the following:
- > It is a line graph with two lines, one yellow and one blue.
 - > The x-axis is labeled with dates from Wed, Apr 4, 2018 to Tue, Apr 10, 2018.
 - > The y-axis is labeled with numbers from 0 to 15.
 - > The yellow line represents "skipped" and the blue line represents "success".
 - > The yellow line has a steady increase from 0 to 15, while the blue line has a sharp increase from 0 to 5, then a decrease to 0, and then a sharp increase to 10.
 - > The graph is titled "Type". Therefore, option C is the correct answer.

NEW QUESTION 215

- (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 219

- (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 220

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 223

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 226

- (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 227

- (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 230

- (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 233

- (Exam Topic 2)

Which of the following are valid options with the chart command

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

Answer: AB

NEW QUESTION 238

- (Exam Topic 2)

The time range specified for a historical search defines the _____, which is 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 range. A historical search is a search that runs over a fixed period of time in the past. When you run a historical search, Splunk searches the index for events that match your search string and fall within the specified time range. 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 241

- (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 command. The transaction command is used to group events that share a common value for one or more fields into transactions. 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 transaction. This limit can be changed by using the maxevents parameter, but it can affect the performance and memory usage of Splunk. 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 246

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

SPLK-1002 Practice Exam Features:

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

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