

Exam Questions SPLK-1002

Splunk Core Certified Power User Exam

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



NEW QUESTION 1

- (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 2

- (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 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 searches will return events contains a tag name Privileged?

- A. Tag= Priv
- B. Tag= Pri*
- C. Tag= Priv*
- D. Tag= Privileged

Answer: B

Explanation:

Reference: <https://docs.splunk.com/Documentation/PCI/4.1.0/Install/PrivilegedUserActivity>

A tag is a descriptive label that you can apply to one or more fields or field values in your events¹. You can use tags to simplify your searches by replacing long or complex field names or values with short and simple tags¹. To search for events that contain a tag name, you can use the tag keyword followed by an equal sign and the tag name¹. You can also use wildcards (*) to match partial tag names¹. Therefore, option B is correct because it will return events that contain a tag name that starts with Pri. Options A and D are incorrect because they will only return events that contain an exact tag name match. Option C is incorrect because it will return events that contain a tag name that starts with Priv, not Privileged.

NEW QUESTION 5

- (Exam Topic 1)

What is required for a macro to accept three arguments?

- A. The macro's name ends with (3).
- B. The macro's name starts with (3).

- C. The macro's argument count setting is 3 or more.
- D. Nothing, all macros can accept any number of arguments.

Answer: A

Explanation:

To create a macro that accepts arguments, you must include the number of arguments in parentheses at the end of the macro name¹. For example, my_macro(3) is a macro that accepts three arguments. The number of arguments in the macro name must match the number of arguments in the definition¹. Therefore, option A is correct, while options B, C and D are incorrect.

NEW QUESTION 6

- (Exam Topic 1)

Which of the following Statements about macros is true? (select all that apply)

- A. Arguments are defined at execution time.
- B. Arguments are defined when the macro is created.
- C. Argument values are used to resolve the search string at execution time.
- D. Argument values are used to resolve the search string when the macro is created.

Answer: BC

Explanation:

A macro is a way to save a commonly used search string as a variable that you can reuse in other searches¹. When you create a macro, you can define arguments that are placeholders for values that you specify at execution time¹. The argument values are used to resolve the search string when the macro is invoked, not when it is created¹. Therefore, statements B and C are true, while statements A and D are false.

NEW QUESTION 7

- (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 8

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 9

- (Exam Topic 1)

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 10

- (Exam Topic 1)

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

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

Answer: ABC

Explanation:

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

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. Data models can be composed of one or more of the following datasets:

Events datasets: These are the base datasets that represent raw events in Splunk. Events datasets can be filtered by constraints, such as search terms, sourcetypes, indexes, etc.

Search datasets: These are derived datasets that represent the results of a search on events or other datasets. Search datasets can use any search command, such as stats, eval, rex, etc., to transform the data.

Transaction datasets: These are derived datasets that represent groups of events that are related by fields, time, or both. Transaction datasets can use the transaction command or event types with transactiontype=true to create transactions.

NEW QUESTION 10

- (Exam Topic 1)

Which group of users would most likely use pivots?

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

Answer: A

Explanation:

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

A pivot is a tool that allows you to create reports and dashboards using data models without writing any SPL commands². You can use pivots to explore, filter, split and visualize your data using a graphical

interface². Pivots are designed for users who want to analyze and report on their data without having to learn the SPL syntax or the underlying structure of the data². Therefore, option A is correct, while options B, C and D are incorrect because they are not the typical group of users who would use pivots.

NEW QUESTION 14

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

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

```
sessiontracker(2)
```

The macro definition does the following:

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

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

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

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

NEW QUESTION 19

- (Exam Topic 1)

Calculated fields can be based on which of the following?

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

Answer: B

Explanation:

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

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

NEW QUESTION 21

- (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 25

- (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 26

- (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 27

- (Exam Topic 1)

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

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

Answer: ABD

Explanation:

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

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

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

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

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

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

NEW QUESTION 28

- (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 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)

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 39

- (Exam Topic 1)

What are the two parts of a root event dataset?

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

Answer: C

Explanation:

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

NEW QUESTION 44

- (Exam Topic 1)

Which of the following describes the Splunk Common Information Model (CIM) add-on?

- A. The CIM add-on uses machine learning to normalize data.
- B. The CIM add-on contains dashboards that show how to map data.
- C. The CIM add-on contains data models to help you normalize data.
- D. The CIM add-on is automatically installed in a Splunk environment.

Answer: C

Explanation:

The Splunk Common Information Model (CIM) add-on is a Splunk app that contains data models to help you normalize data from different sources and formats. The CIM add-on defines a common and consistent way of naming and categorizing fields and events in Splunk. This makes it easier to correlate and analyze data across different domains, such as network, security, web, etc. The CIM add-on does not use machine learning to normalize data, but rather relies on predefined field names and values. The CIM add-on does not contain dashboards that show how to map data, but rather provides documentation and examples on how to use the data models. The CIM add-on is not automatically installed in a Splunk environment, but rather needs to be downloaded and installed from Splunkbase.

NEW QUESTION 46

- (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 48

- (Exam Topic 2)

Field aliases are used to _____ data

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

Answer: D

NEW QUESTION 50

- (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 success1.

NEW QUESTION 54

- (Exam Topic 2)

Given the following eval statement:

...| eval field1 - if(isnotnull(field1),field1,0), field2 = if(isnull<field2>, "NO-VALUE", field2) Which of the following is the equivalent using fillnull?

- A. There is no equivalent expression using fillnull
- B. ... | fillnull values=(0,"NO-VALUE") fields=(field1,field2)
- C. ... | fillnull value=0 field1 | fillnull fields
- D. ... | fillnull field1 | fillnull value="NO-VALUE" field2

Answer: B

Explanation:

The fillnull command replaces null values in one or more fields with a specified value. The values option allows you to specify a comma-separated list of values to fill the null values in the corresponding fields. The fields option allows you to specify a comma-separated list of fields to apply the fillnull command to. The eval statement in the question uses the if and isnull functions to check if field1 and field2 have null values and replace them with 0 and "NO-VALUE" respectively. The equivalent expression using fillnull is to use the values option to specify 0 and "NO-VALUE" and the fields option to specify field1 and field2

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

NEW QUESTION 56

- (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 57

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 60

- (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 65

- (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 67

- (Exam Topic 2)

The Splunk Common Information Model (CIM) is a collection of what type of knowledge object?

- A. KV Store
- B. Lookups
- C. Saved searches
- D. Data models

Answer: D

Explanation:

The Splunk Common Information Model (CIM) is a collection of data models that apply a common structure and naming convention to data from any source. A data model is a type of knowledge object that defines the structure and relationships of fields in a dataset. A data model can have one or more datasets, which are subsets of the data model that represent different aspects of the data. For example, the Network Traffic data model has datasets such as All Traffic, DNS, HTTP, etc. The CIM contains 28 pre-configured data models that cover various domains such as authentication, network traffic, web, email, etc. The CIM is implemented as an add-on that contains the JSON files for the data models, documentation, and tools that support the consistent, normalized treatment of data for maximum efficiency at search time²³

1: Splunk Core Certified Power User Track, page 10. 2: Splunk Documentation, Overview of the Splunk Common Information Model 1. 3: Splunkbase, Splunk Common Information Model (CIM) 2.

NEW QUESTION 71

- (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 72

- (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 73

- (Exam Topic 2)

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

- A. | eval host = if (isnull (src), src, host)
- B. | eval host = if (NOT src = host, src, host)
- C. | eval host = if (src = host, src, host)
- D. | eval host = if (isnotnull (src), src, host)

Answer: D

Explanation:

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

NEW QUESTION 78

- (Exam Topic 2)

Which type of visualization shows relationships between discrete values in three dimensions?

- A. Pie chart
- B. Line chart
- C. Bubble chart
- D. Scatter chart

Answer: C

Explanation:

<https://docs.splunk.com/Documentation/DashApp/0.9.0/DashApp/chartsBub>

NEW QUESTION 82

- (Exam Topic 2)

When would a user select delimited field extractions using the Field Extractor (FX)?

- A. When a log file has values that are separated by the same character, for example, commas.
- B. When a log file contains empty lines or comments.
- C. With structured files such as JSON or XML.
- D. When the file has a header that might provide information about its structure or format.

Answer: A

Explanation:

The correct answer is A. When a log file has values that are separated by the same character, for example, commas.

The Field Extractor (FX) is a utility in Splunk Web that allows you to create new fields from your events by using either regular expressions or delimiters. The FX provides a graphical interface that guides you through the steps of defining and testing your field extractions¹.

The FX supports two field extraction methods: regular expression and delimited. The regular expression method works best with unstructured event data, such as logs or messages, that do not have a consistent format or structure. You select a sample event and highlight one or more fields to extract from that event, and the FX generates a regular expression that matches similar events in your data set and extracts the fields from them¹.

The delimited 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, a tab, or a space. You select a sample event, identify the delimiter, and then rename the fields that the FX finds¹.

Therefore, you would select the delimited field extraction method when you have a log file that has values that are separated by the same character, for example, commas. This method will allow you to easily extract the fields based on the delimiter without writing complex regular expressions.

The other options are not correct because they are not suitable for the delimited field extraction method. These options are:

- B. When a log file contains empty lines or comments: This option does not indicate that the log file has a structured format or a common delimiter. The delimited method might not work well with this type of data, as it might miss some fields or include some unwanted values.
- C. With structured files such as JSON or XML: This option does not require the delimited method, as Splunk can automatically extract fields from JSON or XML files by using indexed extractions or search-time extractions². The delimited method might not work well with this type of data, as it might not recognize the nested structure or the special characters.
- D. When the file has a header that might provide information about its structure or format: This option does not indicate that the file has a common delimiter between the fields. The delimited method might not work well with this type of data, as it might not be able to identify the fields based on the header information.

References:

- Build field extractions with the field extractor
- Configure indexed field extraction

NEW QUESTION 86

- (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 87

- (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 `fail`². 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 92

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 96

- (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. uses the `table` command to improve performance
- C. limits the fields are extracted
- D. returns a table with 3 columns

Answer: C

NEW QUESTION 100

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 103

- (Exam Topic 2)

Complete the search, `.... | _____ failure>successes`

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

Answer: B

Explanation:

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

`... | where failure>successes`

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

The search string below does the following:

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

NEW QUESTION 107

- (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 112

- (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 116

- (Exam Topic 2)

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

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

Answer: AC

Explanation:

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

NEW QUESTION 120

- (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 125

- (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 127

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

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

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

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

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

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

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

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

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

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

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

References:

- Splxicon:Workflowaction
- About workflow actions in Splunk Web

NEW QUESTION 130

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 131

- (Exam Topic 2)

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

- A. Calculated fields cannot be chained together to create more complex fields
- B. Calculated fields can be chained together to create more complex fields.
- C. Calculated fields can only be used in dashboards.
- D. Calculated fields can only be used in saved reports.

Answer: B

Explanation:

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

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

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

```
discount = total * 0.9
```

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

- > About calculated fields
- > Chaining calculated fields

NEW QUESTION 134

- (Exam Topic 2)

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

- A. users
- B. power users
- C. administrators

Answer: BC

NEW QUESTION 137

- (Exam Topic 2)

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

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

Answer: B

Explanation:

The correct answer is B. Event category tags. This is because the CIM add-on contains a collection of preconfigured data models that you can apply to your data at search time. Each data model in the CIM consists of a set of field names and tags that define the least common denominator of a domain of interest. Event category tags are used to classify events into high-level categories, such as authentication, network traffic, or web activity. You can use these tags to filter and analyze events based on their category. You can learn more about event category tags from the Splunk documentation¹². The other options are incorrect because they are not included with the CIM add-on. Search macros are reusable pieces of search syntax that you can invoke from other searches. They are not specific to the CIM add-on, although some Splunk apps may provide their own search macros. Workflow actions are custom links or scripts that you can run on specific fields or events. They are also not specific to the CIM add-on, although some Splunk apps may provide their own workflow actions. tsidx files are index files that store the terms and pointers to the raw data in Splunk buckets. They are part of the Splunk indexing process and have nothing to do with the CIM add-on.

NEW QUESTION 142

- (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 143

- (Exam Topic 2)

When is a GET workflow action needed?

- A. To send field values to an external resource.

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

Answer: B

NEW QUESTION 145

- (Exam Topic 2)

Tags can reference which of the following knowledge objects?

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

Answer: B

Explanation:

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

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

NEW QUESTION 148

- (Exam Topic 2)

By default search results are not returned in _____ order.

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

Answer: AD

NEW QUESTION 153

- (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)

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 158

- (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 159

- (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 results². 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 pairs². The fields sidebar only shows 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 fields are fields that appear in at least 20 percent of events or have high variability among values². 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 163

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 164

- (Exam Topic 2)

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

- A. True
- B. False

Answer: A

NEW QUESTION 165

- (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 167

- (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 170

- (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 175

- (Exam Topic 2)

The stats command will create a _____ by default.

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

Answer: A

NEW QUESTION 180

- (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)

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 188

- (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 192

- (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 195

- (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 200

- (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 201

- (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 203

- (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 204

- (Exam Topic 2)

Clicking a SEGMENT on a chart, _____.

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

Answer: C

NEW QUESTION 205

- (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 208

- (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 213

- (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 218

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 220

.....

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