Splunk

Exam Questions SPLK-1002

Splunk Core Certified Power User Exam

NEW QUESTION 1
- (Exam Topic 1)
What does the fillnull command replace null values with, it 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-specfying-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 2
- (Exam Topic 1)
Which of the following actions can the eval command perform?

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

Answer: B

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

NEW QUESTION 3
- (Exam Topic 1)
In which of the following scenarios is an event type more effective than a saved search?

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

Answer: C

Explanation:
Reference: https://answers.splunk.com/answers/4993/eventtype-vs-saved-search.html
An event type is a way to categorize events based on a search string that matches the events2. You can use event types to simplify your searches by replacing long or complex search strings with short and simple event type names2. An event type is more effective than a saved search when the search string needs to be used in future searches because it allows you to reuse the search string without having to remember or type it again2. Therefore, option C is correct, while options A, B and D are incorrect because they are not scenarios where an event type is more effective than a saved search.

NEW QUESTION 4
- (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: : <fieldneme>

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 5
- (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 6
- (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 7
- (Exam Topic 1)
Which of the following statements describes Search workflow actions?

A. By defaul
B. Search workflow actions will run as a real-time search.
C. Search workflow actions can be configured as scheduled searches,
D. The user can define the time range of the search when created the workflow action.
E. Search workflow actions cannot be configured with a search string that includes the transaction command

Answer: C

Explanation:
Search workflow actions are custom actions that run a search when you click on a field value in your search results. Search workflow actions can be configured with various options, such as label name, search string, time range, app context, etc. One of the options is to define the time range of the search when creating the workflow action. You can choose from predefined time ranges, such as Last 24 hours, Last 7 days, etc., or
specify a custom time range using relative or absolute time modifiers. Search workflow actions do not run as real-time searches by default, but rather use the same time range as the original search unless specified otherwise. Search workflow actions cannot be configured as scheduled searches, as they are only triggered by user interaction. Search workflow actions can be configured with any valid search string that includes any search command, such as transaction.

NEW QUESTION 8
- (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 9
- (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 10
- (Exam Topic 1)
Which of the following knowledge objects represents the output of an eval expression?

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

Answer: B

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

NEW QUESTION 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 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 filed 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 startime.

Therefore, the statements B, C, and D are true.

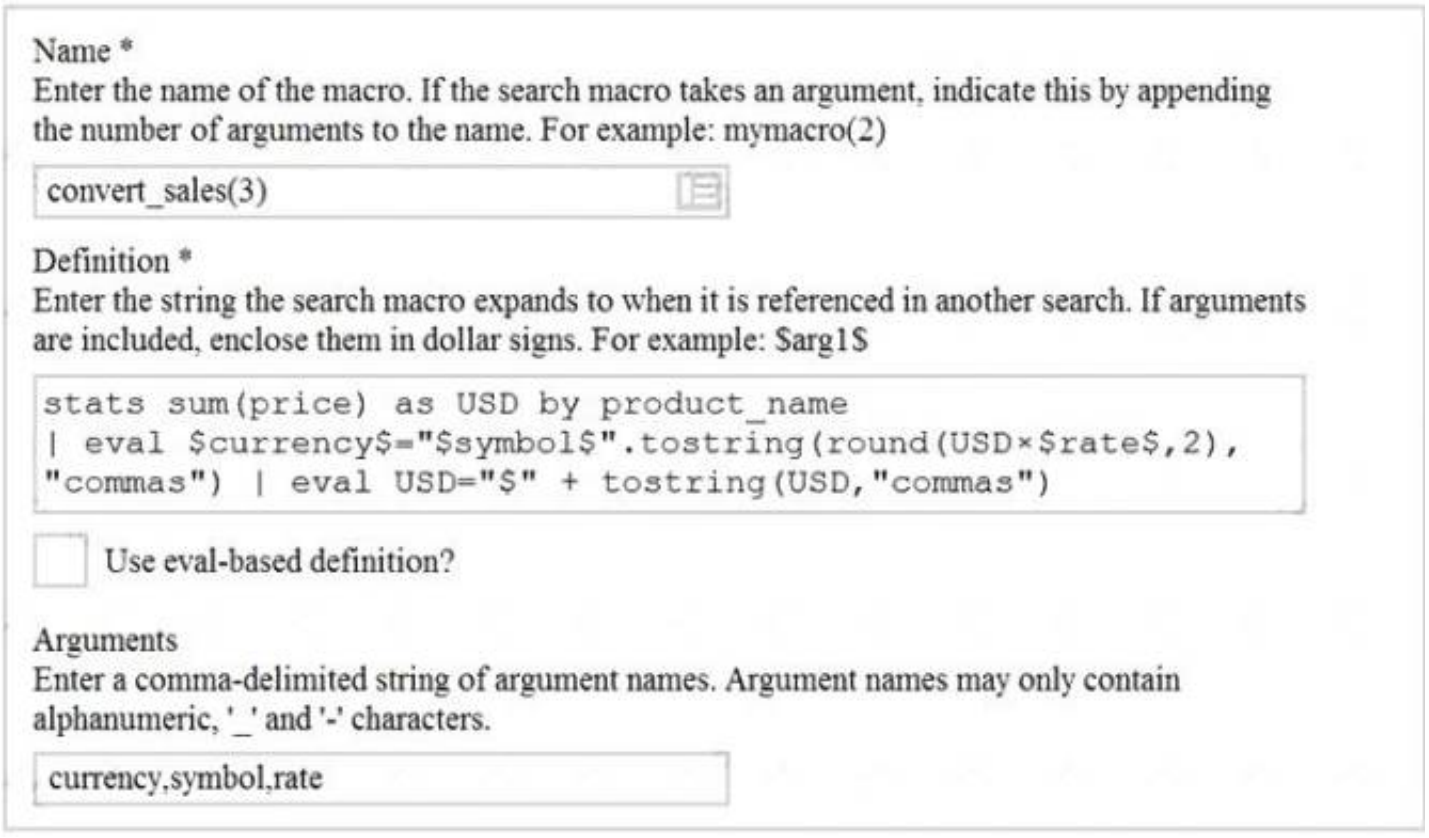
NEW QUESTION 16
- (Exam Topic 1)
Which group of users would most likely use pivots?

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

Answer: A

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Pivot/IntroductiontoPivot
A pivot is a tool that allows you to create reports and dashboards using data models without writing any SPL commands2. You can use pivots to explore, filter, split and visualize your data using a graphical
interface2. Pivots are designed for users who want to analyze and report on their data without having to learn the SPL syntax or the underlying structure of the data2. Therefore, option A is correct, while options B, C and D are incorrect because they are not the typical group of users who would use pivots.

NEW QUESTION 19
- (Exam Topic 1)
Based on the macro definition shown below, what is the correct way to execute the macro in a search string?



A. Convert_sales (euro, €, 79)”
B. Convert_sales (euro, €, .79)
C. Convert_sales ($euro,$€$,s79$
D. Convert_sales ($euro, $€$,S,79$)

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Usesearchmacros
The correct way to execute the macro in a search string is to use the format macro_name($arg1$, $arg2$,
...) where $arg1$, $arg2$, etc. are the arguments for the macro. In this case, the macro name
is convert_sales and it takes three arguments: currency, symbol, and rate. The arguments are enclosed i signs and separated by commas. Therefore, the correct way to execute the macro is convert_sales($euro$, $€$
.79).

NEW QUESTION 24
- (Exam Topic 1)
A calculated field maybe based on which of the following?

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

Answer: B

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

NEW QUESTION 25
- (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 27
- (Exam Topic 1)
Which of the following statements describe data model acceleration? (select all that apply)

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

Answer: BCD

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

NEW QUESTION 31
- (Exam Topic 1)
In what order arc the following knowledge objects/configurations applied?

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

Answer: B

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

NEW QUESTION 34
- (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 39
- (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 43
- (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 44
- (Exam Topic 1)
Which of the following statements describe the search below? (select all that apply) Index=main I 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, startime, etc. The

duration field shows the time span between the first and last events in a transaction.

NEW QUESTION 47
- (Exam Topic 1)
When performing a regular expression (regex) field extraction using the Field Extractor (FX), what happens when the require option is used?

A. The regex can no longer be edited.
B. The field being extracted will be required for all future events.
C. The events without the required field will not display in searches.
D. Only events with the required string will be included in the extraction.

Answer: D

Explanation:
The Field Extractor (FX) allows you to use regular expressions (regex) to extract fields from your events using a graphical interface or by manually editing the regex2. When you use the FX to perform a regex field extraction, you can use the require option to specify a string that must be present in an event for it to be included in the extraction2. This way, you can filter out events that do not contain the required string and focu on the events that are relevant for your extraction2. Therefore, option D is correct, while options A, B and C are incorrect.

NEW QUESTION 50
- (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 53
- (Exam Topic 1)
What does the following search do?

```
index=corndog type=mysterymeat action=eaten | stats count as corndog_count by user
```

A. Creates a table of the total count of users and split by corndogs.
B. Creates a table of the total count of mysterymeat corndogs split by user.
C. Creates a table with the count of all types of corndogs eaten split by user.
D. Creates a table that groups the total number of users by vegetarian corndogs.

Answer: B

Explanation:
The search string below creates a table of the total count of mysterymeat corndogs split by user.
| stats count by user | where corndog=mysterymeat The search string does the following:

- It uses the stats command to calculate the count of events for each value of the user field. The stats command creates a table with two columns: user and count.
- It uses the where command to filter the results by the value of the corndog field. The where command only keeps the rows where corndog equals mysterymeat.

Therefore, the search string creates a table of the total count of mysterymeat corndogs split by user.

NEW QUESTION 58
- (Exam Topic 1)
Which one of the following statements about the search command is true?

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

Answer: D

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

NEW QUESTION 62
- (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 65
- (Exam Topic 1)
Which of the following file formats can be extracted using a delimiter field extraction?

A. CSV
B. PDF
C. XML
D. JSON

Answer: A

Explanation:

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

NEW QUESTION 67
- (Exam Topic 1)
What does the Splunk Common Information Model (CIM) add-on include? (select all that apply)

A. Custom visualizations
B. Pre-configured data models
C. Fields and event category tags
D. Automatic data model acceleration

Answer: BC

Explanation:
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 pre-configured data models that cover various domains such as Alerts, Email, Database, Network Traffic, Web and more3. Therefore, option B is correct. The CIM add-on also includes fields and event category tags that define the common attributes and labels for the data models3. Therefore, option C is correct. The CIM add-on does not include custom visualizations or automatic data model acceleration. Therefore, options A and D are incorrect.

NEW QUESTION 72
- (Exam Topic 1)
When creating a Search workflow action, which field is required?

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

Answer: A

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Setupasearchworkflowaction A workflow action is a link that appears when you click an event field value in your search results2. A
workflow action can open a web page or run another search based on the field value2. There are two types of workflow actions: GET and POST2. A GET workflow action appends the field value to the end of a URI and opens it in a web browser2. A POST workflow action sends the field value as part of an HTTP request to a web server2. When creating a Search workflow action, which is a type of GET workflow action that runs another search based on the field value, the only required field is the search string2. The search string defines the search that will be run when the workflow action is clicked2. Therefore, option A is correct, while options B, C and D are incorrect because they are not required fields for creating a Search workflow action.

NEW QUESTION 75
- (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 80
- (Exam Topic 2)
A field alias is created where field1—fieid2 and the Overwrite Field Values checkbox is selected. What happens if an event only contains values for fieid1?

A. field2 values are removed from the events.
B. field1 and field2 values are merged.
C. field2 values are unchanged.
D. field2 values are replaced with the value of the field1.

Answer: D

Explanation:
The correct answer is D. field2 values are replaced with the value of the field1.
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 convenience1.
When you create a field alias in Splunk Web, you can select the Overwrite Field Values option to change the behavior of the field alias. This option affects how the Splunk software handles situations where the original field has no value or does not exist, as well as situations where the alias field already exists as a field in your events, alongside the original field2.
If you select the Overwrite Field Values option, the following rules apply:

- If the original field does not exist or has no value in an event, the alias field is removed from that event.
- If the original field and the alias field both exist in an event, the value of the alias field is replaced with the value of the original field.

If you do not select the Overwrite Field Values option, the following rules apply:

- If the original field does not exist or has no value in an event, the alias field is unchanged in that event.
- If the original field and the alias field both exist in an event, both fields are retained with their respective values.

Therefore, if you create a field alias where field1—field2 and select the Overwrite Field Values option, and an event only contains values for field1, then the value of field2 will be replaced with the value of field1. References:

- About calculated fields
- About field aliases
- Create field aliases in Splunk Web

NEW QUESTION 83
- (Exam Topic 2)
Which of the following search modes automatically returns all extracted fields in the fields sidebar?

A. Fast
B. Smart
C. Verbose

Answer: C

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

NEW QUESTION 88
- (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 89
- (Exam Topic 2)
When using the transaction command, how are evicted transactions identified?

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

Answer: A

Explanation:

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

NEW QUESTION 93

- (Exam Topic 2)
What type of command is eval?

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

Answer: C

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

NEW QUESTION 97
- (Exam Topic 2)
What are the expected results for a search that contains the command | where A=B?

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

Answer: C

Explanation:
The correct answer is C. Events where values of field A are equal to values of field B.
The where command is used to filter the search results based on an expression that evaluates to true or false. The where command can compare two fields, two values, or a field and a value. The where command can also use functions, operators, and wildcards to create complex expressions1.
The syntax for the where command is:
| where <expression>
The expression can be a comparison, a calculation, a logical operation, or a combination of these. The expression must evaluate to true or false for each event.
To compare two fields with the where command, you need to use the field names without any quotation marks. For example, if you want to find events where the values for the field A match the values for the field
B, you can use the following syntax:
| where A=B
This will return only the events where the two fields have the same value.
The other options are not correct because they use different syntax or fields that are not related to the where command. These options are:

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

References:

- where command usage
- Search command cheatsheet

NEW QUESTION 99
- (Exam Topic 2)
Field aliases are used to _____ data

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

Answer: D

NEW QUESTION 103
- (Exam Topic 2)
Given the following eval statement:
...| eval fieldl - if(isnotnull(fieldl),fieldl,0), field2 = if(isnull<field2>, "NO-VALUE", fieid2) Which of the following is the equivalent using f ilinull?

A. There is no equivalent expression using f ilinull
B. ... t filinull values=(0,"NO-VALUE") fields=(fieldl,field2)
C. ... I filinull value=0 fieldl I fillnull fields
D. ... I fillnull fieldl I filinull 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 field22
1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, fillnull command.

NEW QUESTION 107
- (Exam Topic 2)
Which field extraction method should be selected for comma-separated data?

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

Answer: B

Explanation:
The correct answer is B. Delimiters. This is because the delimiters method is designed for structured event data, such as data from files with headers, where all of the fields in the events are separated by a common delimiter, such as a comma or space. You can select a sample event, identify the delimiter, and then rename the fields that the field extractor finds. You can learn more about the delimiters method from the Splunk documentation1. The other options are incorrect because they are not suitable for comma-separated data. The regular expression method works best with unstructured event data, where you select and highlight one or more fields to extract from a sample event, and the field extractor generates a regular expression that matches similar events and extracts the fields from them. The eval expression is a command that lets you calculate new fields or modify existing fields using arithmetic, string, and logical operations. The table extraction is a feature that lets you extract tabular data from PDF files or web pages. You can learn more about these methods from the Splunk documentation23 .

NEW QUESTION 111
- (Exam Topic 2)
Using the export function, you can export search results as _____ .(Select all that apply)

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

Answer: AB

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

NEW QUESTION 115
- (Exam Topic 2)
A user runs the following search:
index—X sourcetype=Y I 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 118
- (Exam Topic 2)
The macro weekly_sales (2) contains the search string:
index—games I eval Product Sales = $price$ $AmountS01d$ 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 123
- (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 124
- (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 125
- (Exam Topic 2)
Consider the the following search run over a time range of last 7 days: index=web sourcetype=access_conbined | timechart avg(bytes) by product_nane
Which option is used to change the default time span so that results are grouped into 12 hour intervals?

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

Answer: A

Explanation:
The span option is used to specify the time span for the timechart command. The span value can be a number followed by a time unit, such as h for hour, d for day, w for week, etc. The span value determines how the data is grouped into time buckets. For example, span=12h means that the data is grouped into 12-hour intervals. The timespan option is not a valid option for the timechart command2
1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, timechart command.

NEW QUESTION 130
- (Exam Topic 2)
Which statement is true?

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

Answer: C

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Pivot/IntroductiontoPivot
Pivot is used for creating reports and dashboards. Pivot is a tool that allows you to create reports and dashboards from your data models without writing any SPL commands. Pivot can help you visualize and analyze your data using various options, such as filters, rows, columns, cells, charts, tables, maps, etc. Pivot can also help you accelerate your reports and dashboards by using summary data from your accelerated data models.
Pivot is not used for creating datasets or data models. Datasets are collections of events that represent your data in a structured and hierarchical way. Data models are predefined datasets for various domains, such as network traffic, web activity, authentication, etc. Datasets and data models can be created by using commands such as datamodel or pivot.

NEW QUESTION 131
- (Exam Topic 2)
Which workflow action method can be used the action type is set to link?

A. GET
B. PUT

C. Search
D. UPDATE

Answer: A

Explanation:

https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/SetupaGETworkflowaction
Define a GET workflow action
Steps

- Navigate to Settings > Fields > Workflow Actions.
- Click New to open up a new workflow action form.
- Define a Label for the action.

The Label field enables you to define the text that is displayed in either the field or event workflow menu.
Labels can be static or include the value of relevant fields.

- Determine whether the workflow action applies to specific fields or event types in your data.

Use Apply only to the following fields to identify one or more fields. When you identify fields, the workflow action only appears for events that have those fields, either in their event menu or field menus. If you leave it blank or enter an asterisk the action appears in menus for all fields.
Use Apply only to the following event types to identify one or more event types. If you identify an event type, the workflow action only appears in the event menus for events that belong to the event type.

- For Show action in determine whether you want the action to appear in the Event menu, the Fields menus, or Both.
- Set Action type to link.
- In URI provide a URI for the location of the external resource that you want to send your field values to.

Similar to the Label setting, when you declare the value of a field, you use the name of the field enclosed by dollar signs.
Variables passed in GET actions via URIs are automatically URL encoded during transmission. This means you can include values that have spaces between words or punctuation characters.

- Under Open link in, determine whether the workflow action displays in the current window or if it opens the link in a new window.
- Set the Link method to get.
- Click Save

to save your workflow action definition.

NEW QUESTION 133
- (Exam Topic 2)
Which of the following eval commands will provide a new value for host from src if it exists?

A. | eval host = if (isnu11 (src), src, host)
B. | eval host = if (NOT src = host, src, host)
C. | eval host = if (src = host, src, host)
D. | eval host = if (isnotnull (src), src, host)

Answer: D

Explanation:

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

NEW QUESTION 138
- (Exam Topic 2)
Which of the following statements describes calculated fields?

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

Answer: B

NEW QUESTION 143
- (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 145
- (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 149
- (Exam Topic 2)
For the following search, which field populates the x-axis? index=security sourcetype=linux secure | timechart count by action

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

Answer: C

Explanation:
The correct answer is C. _time.
The timechart command creates a time series chart with corresponding table of statistics, with time used as the X-axis1. You can specify a split-by field, where each distinct value of the split-by field becomes a series in the chart1. In this case, the split-by field is action, which means that the chart will have different lines for different actions, such as accept, reject, or fail2. The count function will calculate the number of events for each action in each time bin1.
For example, the following image shows a timechart of the count by action for a similar search3:
As you can see, the x-axis is populated by the _time field, which represents the time range of the search. The y-axis is populated by the count function, which represents the number of events for each action. The legend shows the different values of the action field, which are used to split the chart into different series.
Reference:
2: Timechart Command In Splunk With Example - Mindmajix 1: timechart - Splunk Documentation 3: timechart command examples - Splunk Documentation

NEW QUESTION 154
- (Exam Topic 2)
Which of the following statements describes the use of the Field Extractor (FX)?

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

Answer: C

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

NEW QUESTION 155
- (Exam Topic 2)
Which of the following eval command functions is valid?

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

Answer: D

Explanation:
https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/CommonEvalFunctions
The eval command function tostring() is valid. The tostring() function converts a numeric value to a string value. For example, tostring(3.14) returns “3.14”. The other functions are not valid eval command functions.

NEW QUESTION 160
- (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 164
- (Exam Topic 2)
In which Settings section are macros defined?

A. Fields
B. Tokens
C. Advanced Search
D. Searches, Reports, Alerts

Answer: C

NEW QUESTION 169
- (Exam Topic 2)
How is an event type created from the search window? (select all that apply)

A. In the top right corner, click Save As > Event Type.
B. In an event's detail dropdown, click Event Actions > Build Event Type.
C. Edit eventtypes.conf and add a new stanza.
D. Add | eventtype to the SPL and execute the search.

Answer: AC

Explanation:
In Splunk, you can create an event type from the search window by running a search that would make a good event type, then clicking Save As and selecting Event Type1. This opens the Save as Event Type dial you can provide the event type name and optionally apply tags to it1.
You can also create an event type by editing the eventtypes.conf file and adding a new stanza1. Each stanz the eventtypes.conf file represents an event type1. The stanza name is the name of the event type, and
the search attribute specifies the search string that defines the event type1.
It’s important to note that while you can use the eventtype command in a search to find events associated wit a specific event type, adding | eventtype to the SPL and executing the search does not create a new event type1. Similarly, clicking Event Actions > Build Event Type in an event’s detail dropdown does not create new event type1.

NEW QUESTION 173
- (Exam Topic 2)
These kinds of charts represent a series in a single bar with multiple sections

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

Answer: D

Explanation:
Stacked charts represent a series in a single bar with multiple sections. A chart is a graphical representation of data that shows trends, patterns, or comparisons. A chart can have different types, such as column, bar, line, area, pie, etc. A chart can also have different modes, such as split-series, multi-series, stacked, etc. A stacked chart is a type of chart that shows multiple series in a single bar or area with different sections for each series

NEW QUESTION 177
- (Exam Topic 2)
Which of the following are valid options to speed up reports? (Select all the apply.)

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

Answer: C

Explanation:
One of the valid options to speed up reports is to edit acceleration, which means that you can enable summary indexing or data model acceleration for your reports to improve their performance2. Summary indexing allows you to create reports that run over large amounts of data by storing the results of scheduled searches in a summary index and using that index for faster reporting2. Data model acceleration allows you to create reports that use data models by creating and storing

summaries of the data model datasets and using them for faster reporting2. Therefore, option C is correct, while options A, B and D are incorrect because they are not options to speed up reports.

NEW QUESTION 179
- (Exam Topic 2)
Which of the following is one of the pre-configured data models included in the Splunk Common Information Model (CIM) add-on?

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

Answer: D

NEW QUESTION 180
- (Exam Topic 2)
This function of the stats command allows you to return the sample standard deviation of a field.

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

Answer: A

NEW QUESTION 182
- (Exam Topic 2)
Which search would limit an "alert" tag to the "host" field?

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

Answer: D

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

NEW QUESTION 185
- (Exam Topic 2)
The limit attribute will _____.

A. override default of 10
B. only work with top command
C. override default of 20
D. override default of 15

Answer: A

NEW QUESTION 186
- (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 191
- (Exam Topic 2)
Consider the following search: index=web sourcetype=access_corabined
The log shows several events that share the same jsesszonid value (SD462K101O2F267). View the events as a group.
From the following list, which search groups events by jSSESSIONID?

A. index=web sourcetype=access_combined I transaction JSESSZONID I search SD462K101C2F267
B. index=web sourcetype=access_combined SD462K101O2F267 | table JSESSIONID
C. index=web sourcetype=access_combined | highlight JSESSIONID | search SD462K101O2F267

D. index=web sourcetype=access_combined JSESSTONID <SD4€2K101O2F267>

Answer: A

Explanation:
The transaction command groups events that share a common value in a specified field, such as JSESSIONID, and that occur within a specified time range. The search command filters the results to show only the events that match the given value of JSESSIONID. This search groups the events by JSESSIONID and then shows only the events that have the value SD462K101C2F267 for JSESSIONID2
1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, transaction command.

NEW QUESTION 192
- (Exam Topic 2)
What is a limitation of searches generated by workflow actions?

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

Answer: D

NEW QUESTION 194
- (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 196
- (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 200
- (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 202
- (Exam Topic 2)
What does the fillnull command replace null values with, if the value argument is not specified?

A. N/A
B. NaN
C. NULL

Answer: A

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

NEW QUESTION 206
- (Exam Topic 2)
Which of the following is NOT a stats function:

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

Answer: B

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

NEW QUESTION 209
- (Exam Topic 2)
The stats command will create a _____ by default.

A. Table
B. Report
C. Pie chart

Answer: A

NEW QUESTION 211
- (Exam Topic 2)
Which syntax will find events where the values for the 1 field match the values for the Renewal-MonthYear field?

A. | where 10yearAnnerversary=Renewal-MonthYear
B. | where ‘10yearAnnerversary=Renewal-MonthYear
C. | where 10yearAnnerversary=’Renewal-MonthYear’
D. | where ‘10yearAnnerversary’=’Renewal-MonthYear’

Answer: A

Explanation:
The correct answer is A. | where 10yearAnnerversary=Renewal-MonthYear.
The where command is used to filter the search results based on an expression that evaluates to true or false. The where command can compare two fields, two values, or a field and a value. The where command can also use functions, operators, and wildcards to create complex expressions1.
The syntax for the where command is:
| where <expression>
The expression can be a comparison, a calculation, a logical operation, or a combination of these. The expression must evaluate to true or false for each event.
To compare two fields with the where command, you need to use the field names without any quotation marks. For example, if you want to find events where the values for the 10yearAnnerversary field match the values for the Renewal-MonthYear field, you can use the following syntax:
| where 10yearAnnerversary=Renewal-MonthYear
This will return only the events where the two fields have the same value.
The other options are not correct because they use quotation marks around the field names, which will cause the where command to interpret them as string values instead of field names. For example, if you use:
| where ‘10yearAnnerversary’=‘Renewal-MonthYear’
This will return no events because there are no events where the string value ‘10yearAnnerversary’ is equal to the string value ‘Renewal-MonthYear’.
References:
- where command usage

NEW QUESTION 215
- (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 216
- (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 218
- (Exam Topic 2)
Highlighted search terms indicate _____ search results in Splunk.

A. Display as selected fields.
B. Sorted
C. Charted based on time
D. Matching

Answer: D

Explanation:
Highlighted search terms indicate matching search results in Splunk, which means that they show which parts of your events match your search string2. For example, if you search for error OR fail, Splunk will highlight error or fail in your events to show which events match your search string2. Therefore, option D is correct, while options A, B and C are incorrect because they are not indicated by highlighted search terms.

NEW QUESTION 219
- (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 220
- (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 222
- (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 227
- (Exam Topic 2)
Why would the following search produce multiple transactions instead of one?

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

Events (641) Patterns Statistics (147) Visualization

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

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

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

Answer: A

Explanation:
The correct answer is A. The maxspan option is not included1.
In Splunk, the transaction command is used to group events that share common characteristics into a single transaction1. By default, the transaction command groups all matching events into a single transaction1.
However, you can use the maxspan option to limit the time span of the transactions1. If the time span between the first and last event in a transaction exceeds the maxspan value, the transaction command will start a new transaction1.
Therefore, if the maxspan option is not included in the search, the transaction command might produce multiple transactions instead of one if the time span between the first and last event in a transaction exceeds the default maxspan value1.
Here is an example of how you can use the maxspan option in a search:

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

NEW QUESTION 232
- (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 235
- (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 236
- (Exam Topic 2)
During the validation step of the Field Extractor workflow: Select your answer.

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

Answer: A

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

NEW QUESTION 238
- (Exam Topic 2)
Where are the results of eval commands stored?

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

Answer: A

Explanation:
https://docs.splunk.com/Documentation/Splunk/8.0.2/SearchReference/Eval
The eval command calculates an expression and puts the resulting value into a search results field.
- If the field name that you specify does not match a field in the output, a new field is added to the search results.
- If the field name that you specify matches a field name that already exists in the search results, the results of the eval expression overwrite the values in that field.

NEW QUESTION 242
- (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 243
- (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 246
- (Exam Topic 2)
The time range specified for a historical search defines the _____.------questionable on ans

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

Answer: B

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

NEW QUESTION 247
- (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 251
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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