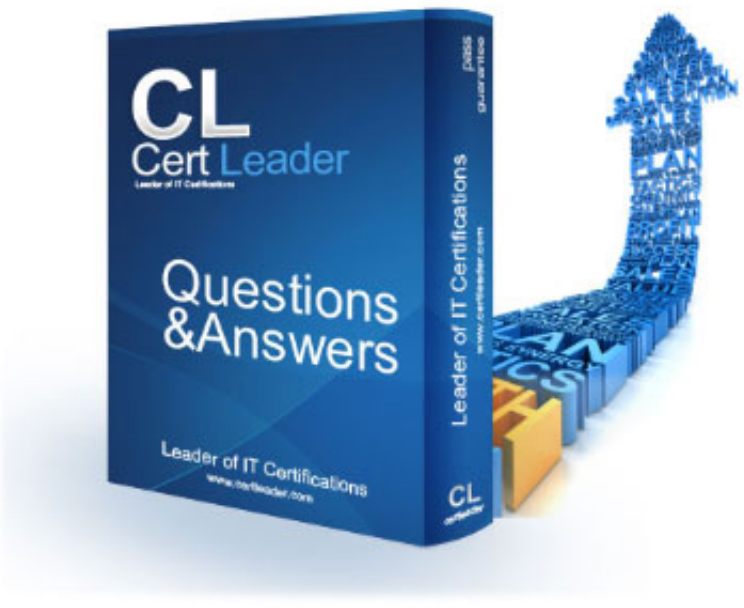
SPLK-1002 Dumps

Splunk Core Certified Power User Exam

https://www.certleader.com/SPLK-1002-dumps.html



NEW QUESTION 1
- (Exam Topic 1)
A space is an implied _____ in a search string.

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

Answer: B

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

NEW QUESTION 2
- (Exam Topic 1)
When multiple event types with different color values are assigned to the same event, what determines the color displayed for the events?

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

Answer: C

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

NEW QUESTION 3
- (Exam Topic 1)
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 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)
Which of the following searches show a valid use of macro? (Select all that apply)

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

Answer: AC

Explanation:
Reference:
https://answers.splunk.com/answers/574643/field-showing-an-additional-and-not-visible-value-1.html
To use a macro in a search, you must enclose the macro name and any arguments in single quotation marks1. For example, 'my_macro(arg1,arg2)' is a valid way to use a macro with two arguments. You can use macro anywhere in your search string where you would normally use a search command or expression1. Therefore, options A and C are valid searches that use macros, while options B and D are invalid because they do not enclose the macros in single quotation marks.

NEW QUESTION 6
- (Exam Topic 1)
Which of the following statements is true, especially in large environments?

A. Use the scats command when you next to group events by two or more fields.
B. The stats command is faster and more efficient than the transaction command
C. The transaction command is faster and more efficient than the stats command.
D. Use the transaction command when you want to see the results of a calculation.

Answer: B

Explanation:
Reference: https://answers.splunk.com/answers/103/transaction-vs-stats-commands.html
The stats command is faster and more efficient than the transaction command, especially in large environments. The stats command is used to calculate summary statistics on the events, such as count, sum, average, etc. The stats command can group events by one or more fields or by time buckets. The stats command does not create new events from groups of events, but rather creates new fields with statistical values. The transaction command is used to group events into transactions based on some common characteristics, such as fields, time, or both. The transaction command creates new events from groups of events that share one or more fields. The transaction command also creates some additional fields for each transaction, such as duration, eventcount, startime, etc. The transaction command is slower and more resource-intensive than the stats command because it has to process more data and create more events and fields.

NEW QUESTION 7
- (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 8
- (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 9
- (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 10
- (Exam Topic 1)
The Field Extractor (FX) is used to extract a custom field. A report can be created using this custom field. The created report can then be shared with other people in the organization. If another person in the organization runs the shared report and no results are returned, why might this be? (select all that apply)

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

Answer: CD

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

NEW QUESTION 10
- (Exam Topic 1)
Which of the following statements describe GET workflow actions?

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

Answer: D

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

NEW QUESTION 11
- (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.

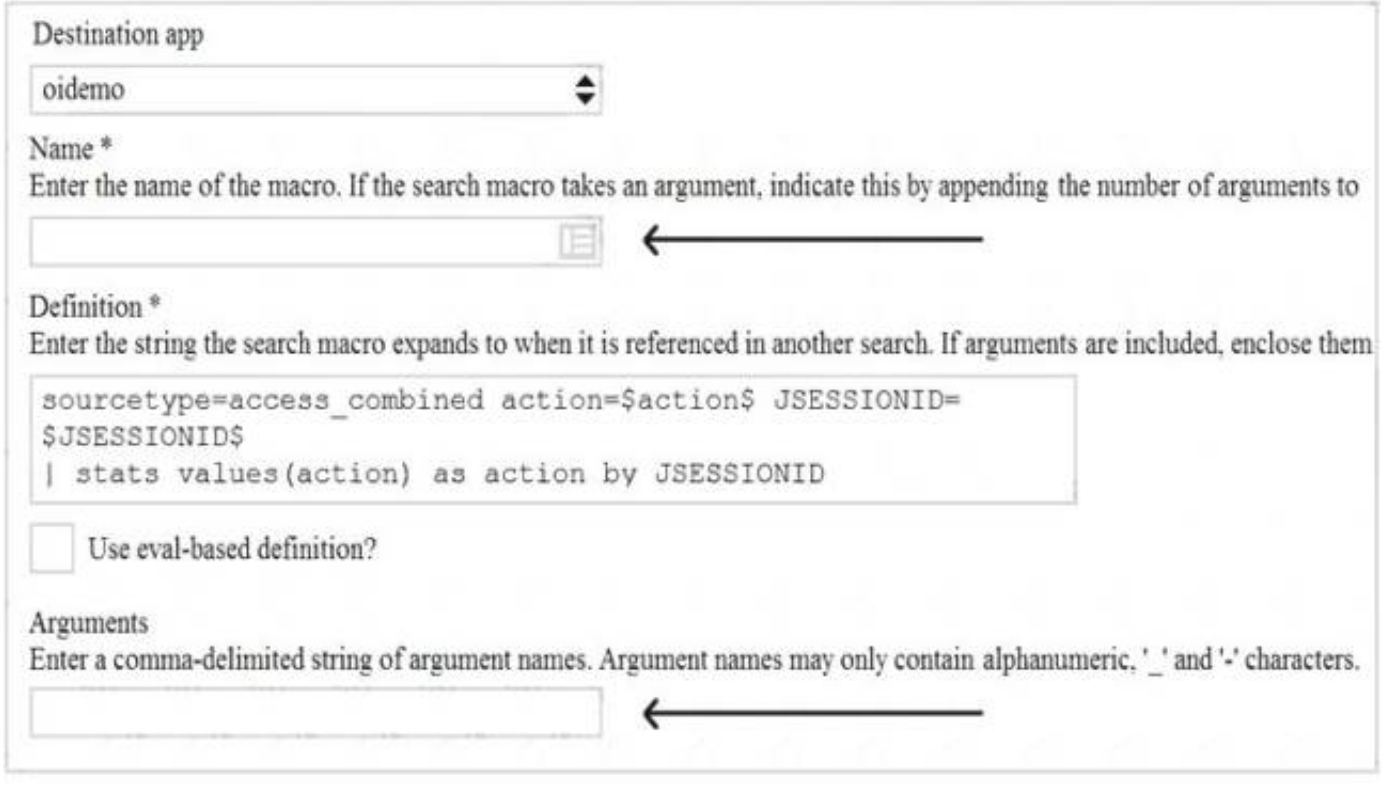
NEW QUESTION 12
- (Exam Topic 1)
Which group of users would most likely use pivots?

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 16
- (Exam Topic 1)
Given the macro definition below, what should be entered into the Name and Arguments fileds to correctly configured the macro?



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

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 21
- (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 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 28
- (Exam Topic 1)
To identify all of the contributing events within a transaction that contains at least one REJECT event, which syntax is correct?

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

Answer: B

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

NEW QUESTION 31
- (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 36
- (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 40
- (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 41
- (Exam Topic 1)
Data model fields can be added using the Auto-Extracted method. Which of the following statements describe Auto-Extracted fields? (select all that apply)

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

Answer: ABCD

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

NEW QUESTION 46
- (Exam Topic 1)
Which of the following workflow actions can be executed from search results? (select all that apply)

A. GET
B. POST
C. LOOKUP
D. Search

Answer: ABD

Explanation:
As mentioned before, there are two types of workflow actions: GET and POST1. Both types of workflow actions can be executed from search results by clicking on an event field value that has a workflow action configured for it1. Another type of workflow action is Search, which runs another search based on the field value1. Therefore, options A, B and D are correct, while option C is incorrect because LOOKUP is not a type of workflow action.

NEW QUESTION 49
- (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 52
- (Exam Topic 1)
Which of the following statements describe calculated fields? (select all that apply)

A. Calculated fields can be used in the search bar.
B. Calculated fields can be based on an extracted field.
C. Calculated fields can only be applied to host and sourcetype.
D. Calculated fields are shortcuts for performing calculations using the eval command.

Answer: ABD

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

Calculated fields are fields that are created by performing calculations on existing fields using the eval command. Calculated fields can be used in the search bar to filter and transform events based on the calculated values. Calculated fields can also be based on an extracted field, which is a field that is extracted from raw data using various methods, such as regex, delimiters, lookups, etc. Calculated fields are not shortcuts for performing calculations using the eval command, but rather results of performing calculations using the eval command. Calculated fields can be applied to any field in Splunk, not only host and sourcetype. Therefore, statements A, B, and D are true about calculated fields.

NEW QUESTION 56
- (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 59
- (Exam Topic 1)
Which of the following statements describe the search string below?
| datamodel Application_State All_Application_State search

A. Evenrches would return a report of sales by state.
B. Events will be returned from the data model named Application_State.
C. Events will be returned from the data model named All_Application_state.
D. No events will be returned because the pipe should occur after the datamodel command

Answer: B

Explanation:
The search string below returns events from the data model named Application_State.
| datamodel Application_State All_Application_State search The search string does the following:

- It uses the datamodel command to access a data model in Splunk. The datamodel command takes two arguments: the name of the data model and the name of the dataset within the data model.
- It specifies the name of the data model as Application_State. This is a predefined data model in Splunk that contains information about web applications.
- It specifies the name of the dataset as All_Application_State. This is a root dataset in the data model that contains all events from all child datasets.
- It uses the search command to filter and transform the events from the dataset. The search command can use any search criteria or command to modify the results.

Therefore, the search string returns events from the data model named Application_State.

NEW QUESTION 63
- (Exam Topic 2)
Which of the following about reports is/are true?

A. Reports are knowledge objects.
B. Reports can be scheduled.
C. Reports can run a script.
D. All of the above.

Answer: D

Explanation:
A report is a way to save a search and its results in a format that you can reuse and share with others2. A report is also a type of knowledge object, which is an entity that you create to add knowledge to your data and make it easier to search and analyze2. Therefore, option A is correct. A report can be scheduled, which means that you can configure it to run at regular intervals and send the results to yourself or others via email or other methods2. Therefore, option B is correct. A report can run a script, which means that you can specify a script file to execute when the report runs and use it to perform custom actions or integrations2. Therefore, option C is correct. Therefore, option D is correct because all of the above statements are true for reports.

NEW QUESTION 65
- (Exam Topic 2)
When using a field value variable with a Workflow Action, which punctuation mark will escape the data

A. *
B. !
C. ^
D. #

Answer: B

Explanation:

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

NEW QUESTION 69
- (Exam Topic 2)
Which of the following searches will show the number of categoryld used by each host?

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

Answer: B

NEW QUESTION 73
- (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 77
- (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 80
- (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 82
- (Exam Topic 2)
Which of the following search control will not re-rerun the search? (Select all that apply.)

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

Answer: BCD

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

NEW QUESTION 85
- (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 89
- (Exam Topic 2)
What fields does the transaction command add to the raw events? (select all that apply)

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

Answer: BD

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

- The transaction command is a Splunk command that finds transactions based on events that meet various constraints12.
- Transactions are made up of the raw text (the _raw field) of each member, the time and date fields of the earliest member, as well as the union of all other fields of each member12.
- The transaction command adds some fields to the raw events that are part of the transaction123. These fields are:
- duration: The difference, in seconds, between the timestamps for the first and last events in the transaction123.
-

eventcount: The number of events in the transaction123.

- transaction_id: A unique identifier for each transaction3. This field is useful for filtering or joining transactions3.
- Therefore, the fields that the transaction command adds to the raw events are duration and transaction_id, which are options B and D in your question.

NEW QUESTION 94
- (Exam Topic 2)
Which command is used to create choropleth maps?

A. geostats
B. cluster
C. geom

Answer: C

NEW QUESTION 95
- (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 97
- (Exam Topic 2)
Information needed to create a GET workflow action includes which of the following? (select all that apply.)

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

Answer: ABC

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/SetupaGETworkflowaction Information needed to create a GET workflow action includes the following: a name of the workflow action, a URI where the user will be directed at search time, and a label that will appear in the Event Action menu at search time. A GET workflow action is a type of workflow action that performs a GET request when you click on a field value in your search results. A GET workflow action can be configured with various options, such as:
A name of the workflow action: This is a unique identifier for the workflow action that is used internally by Splunk. The name should be descriptive and meaningful for the purpose of the workflow action.
A URI where the user will be directed at search time: This is the base URL of the external web service or application that will receive the GET request. The URI can include field value variables that will be replaced by the actual field values at search time. For example, if you have a field value variable ip, you can write it as http://example.com/ip=$ip to send the IP address as a parameter to the external web service or application.
A label that will appear in the Event Action menu at search time: This is the display name of the workflow action that will be shown in the Event Action menu when you click on a field value in your search results. The label should be clear and concise for the user to understand what the workflow action does.
Therefore, options A, B, and C are correct.

NEW QUESTION 99
- (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 104
- (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 107
- (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 112
- (Exam Topic 2)
How are event types different from saved reports?

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

Answer: D

Explanation:
Hello, this is Bing. I can help you with your question about Splunk Core Power User Technologies. The correct answer is D. Event types do not include a time range.
The explanation is as follows:
- Event types are a categorization system that help you make sense of your data by matching events with the same search string1. Event types are applied to events at search time and can be used as search terms or filters12.
- Saved reports are results saved from a search action that can show statistics and visualizations of events3. Saved reports can be run anytime, and they fetch fresh results each time they are run34. Saved reports can be shared with other users and added to dashboards4.
- The main difference between event types and saved reports is that event types do not include a time range, while saved reports do14. This means that event types can match events from any time period, while saved reports are limited by the time range specified when they are created or run14.

NEW QUESTION 116
- (Exam Topic 2)
When using the transaction command, what does the argument maxspan do?

A. Sets the maximum total time between events in a transaction.
B. Sets the maximum length of all events within a transaction.
C. Sets the maximum total time between the earliest and latest events in a transaction.
D. Sets the maximum length that any single event can reach to be included in the transaction.

Answer: C

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

NEW QUESTION 119
- (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 121

- (Exam Topic 2)
What other syntax will produce exactly the same results as | chart count over vendor_action by user?

A. | chart count by vendor_action, user
B. | chart count over vendor_action, user
C. | chart count by vendor_action over user
D. | chart count over user by vendor_action

Answer: A

Explanation:
https://docs.splunk.com/Documentation/Splunk/8.1.2/SearchReference/Chart

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 129
- (Exam Topic 2)
In the Field Extractor Utility, this button will display events that do not contain extracted fields. Select your answer.

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

Answer: B

Explanation:
The Field Extractor Utility (FX) is a tool that helps you extract fields from your events using a graphical interface or by manually editing the regular expression2. The FX has a button that displays events that do not contain extracted fields, which is the Non-Matches button2. The Non-Matches button shows you the events that do not match the regular expression that you have defined for your field extraction2. This way, you can check if your field extraction is accurate and complete2. Therefore, option B is correct, while options A, C and D are incorrect because they are not buttons that display events that do not contain extracted fields.

NEW QUESTION 133
- (Exam Topic 2)
Which of the following commands support the same set of functions?

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

Answer: C

NEW QUESTION 138
- (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 140
- (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 143
- (Exam Topic 2)
Which of these search strings is NOT valid:

A. index=web status=50* | chart count over host, status
B. index=web status=50* | chart count over host by status
C. index=web status=50* | chart count by host, status

Answer: A

Explanation:
This search string is not valid: index=web status=50* | chart count over host,status2. This search string uses an invalid syntax for the chart command. The chart command requires one field after the over clause and optionally one field after the by clause. However, this search string has two fields after the over clause separated by a comma. This will cause a syntax error and prevent the search from running. Therefore, option A is correct, while options B and C are incorrect because they are valid search strings that use the chart command correctly.

NEW QUESTION 144
- (Exam Topic 2)
Which of the following is true about Pivot?

A. Users can save reports from Pivot.
B. Users cannot share visualizations created with Pivot.
C. Users must use SPL to find events in a Pivot.
D. Users cannot create visualizations with Pivot.

Answer: A

Explanation:
In Splunk, Pivot is a tool that allows you to report on a specific data set without using the Splunk Search Processing Language (SPL™)1. You can use a drag-and-drop interface to design and generate pivots that present different aspects of your data in the form of tables, charts, and other visualizations12.
One of the features of Pivot is that it allows you to save your reports1. This can be useful when you want to reuse a report or share it with others1. Therefore, it's not true that users cannot share visualizations created with Pivot or that they must use SPL to find events in a Pivot12. It's also not true that users cannot create visualizations with Pivot, as creating visualizations is one of the main functions of Pivot12.

NEW QUESTION 145
- (Exam Topic 2)
When a search returns _____, you can view the results as a list.

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

Answer: C

NEW QUESTION 149
- (Exam Topic 2)
Which of the following statements are true for this search? (Select all that apply.)
SEARCH: sourcetype=access* |fields action productId status

A. is looking for all events that include the search terms: fields AND action AND productId AND status
B. users the table command to improve performance
C. limits the fields are extracted
D. returns a table with 3 columns

Answer: C

NEW QUESTION 153
- (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 158
- (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 161
- (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 166
- (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 170
- (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 171
- (Exam Topic 2)
Which of the following statements best describes a macro?

A. A macro is a method of categorizing events based on a search.
B. A macro is a way to associate an additional (new) name with an existing field name.
C. A macro is a portion of a search that can be reused in multiple place
D. A macro is a knowledge object that enables you to schedule searches for specific events.

Answer: C

Explanation:
The correct answer is C. A macro is a portion of a search that can be reused in multiple places.
A macro is a way to reuse a piece of SPL code in different searches. A macro can be any part of a search, such as an eval statement or a search term, and does not need to be a complete command. A macro can also take arguments, which are variables that can be replaced by different values when the macro is called. A macro can also contain another macro within it, which is called a nested macro1.
To create a macro, you need to define its name, definition, arguments, and description in the Settings > Advanced Search > Search Macros page in Splunk Web or in the macros.conf file. To use a macro in a search, you need to enclose the macro name in backtick characters (`) and provide values for the arguments if any1.
For example, if you have a macro named my_macro that takes one argument named object and has the following definition:
search sourcetype= object
You can use it in a search by writing: my_macro(web)
This will expand the macro and run the following SPL code: search sourcetype=web
The benefits of using macros are that they can simplify complex searches, reduce errors, improve readability, and promote consistency1.
The other options are not correct because they describe other types of knowledge objects in Splunk, not macros. These objects are:
- A. An event type is a method of categorizing events based on a search. An event type assigns a label to events that match a specific search criteria. Event types can be used to filter and group events, create alerts, or generate reports2.
- B. A field alias is a way to associate an additional (new) name with an existing field name. A field alias can be used to normalize fields from different sources that have different names but represent the same data. Field aliases can also be used to rename fields for clarity or convenience3.
- D. An alert is a knowledge object that enables you to schedule searches for specific events and trigger actions when certain conditions are met. An alert can be used to monitor your data for anomalies, errors, or other patterns of interest and notify you or others when they occur4.

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

NEW QUESTION 175
- (Exam Topic 2)
When using | timechart by host, which field is represented in the x-axis?

A. date
B. host
C. time
D. _time

Answer: D

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.4/SearchReference/Timechart

NEW QUESTION 177
- (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:

- Splexicon:Workflowaction
- About workflow actions in Splunk Web

NEW QUESTION 179
- (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 184
- (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 185
- (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 190
- (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 194
- (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 196
- (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 197
- (Exam Topic 2)
A data model consists of which three types of datasets?

A. Constraint, field, value.
B. Events, searches, transactions.
C. Field extraction, regex, delimited.

D. Transaction, session ID, metadata.

Answer: B

Explanation:
The building block of a data model. Each data model is composed of one or more data model datasets. Each dataset within a data model defines a subset of the dataset represented by the data model as a whole.
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 198
- (Exam Topic 2)
If a calculated field has the same name as an extracted field, what happens to the extracted field?

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

Answer: A

Explanation:
When you define a calculated field, you can specify the name of the field that the eval expression will create or modify. If the name of the calculated field matches the name of an existing extracted field, the calculated field will override the extracted field and replace its value with the result of the eval expression. This means that the original value of the extracted field will not be available for searching or analysis. To avoid this, you should use a unique name for your calculated field or use a different name for your extracted field2
1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, Configure calculated fields with props.conf.

NEW QUESTION 202
- (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 207
- (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 209
- (Exam Topic 2)
Which search string would only return results for an event type called success ful_purchases?

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

Answer: C

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

NEW QUESTION 210
- (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 212
- (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 215
- (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 219
- (Exam Topic 2)
Which is not a comparison operator in Splunk

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

Answer: E

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

NEW QUESTION 220
- (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 224
- (Exam Topic 2) Consider the following search: Index=web sourcetype=access_combined
The log shows several events that share the same JSESSIONID value (SD404K289O2F151). View the events as a group. From the following list, which search groups events by JSESSIONID?

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

Answer: B

NEW QUESTION 229
- (Exam Topic 2)
Which of the following is a function of the Splunk Common Information Model (CIM)?

A. Normalizing data across a Splunk deployment.
B. Providing templates for reports and dashboards.
C. Algorithmically shifting events to other indexes.
D. Reingesting previously indexed data with new field names.

Answer: A

NEW QUESTION 230
- (Exam Topic 2)
Which statement is true?

A. Pivot is used for creating datasets.
B. Data models 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:
The statement that pivot is used for creating reports and dashboards is true. Pivot is a graphical interface that allows you to create tables, charts, and visualizations from data models. Data models are structured datasets that define how data is organized and categorized. Pivot does not create datasets, but uses existing ones.

NEW QUESTION 231
- (Exam Topic 2)
Which of the following is a feature of the Pivot tool?

A. Creates lookups without using SPL.
B. Data Models are not required.
C. Creates reports without using SPL
D. Datasets are not required.

Answer: C

Explanation:
The correct answer is C. Creates reports without using SPL. This is because the Pivot tool is a feature of Splunk that allows you to report on a specific data set without using the Splunk Search Processing Language (SPL). You can use a drag-and-drop interface to design and generate pivots that present different aspects of your data in the form of tables, charts, and other visualizations. You can learn more about the Pivot tool from the Splunk documentation1 or watch a video tutorial2. The other options are incorrect because they do not describe the features of the Pivot tool. The Pivot tool requires data models and datasets to define the data that you want to work with. Data models and datasets are designed by the knowledge managers in your organization. You can learn more about data models and datasets from the Splunk documentation3. The Pivot tool does not create lookups, which are tables that match field values to other field values. You can create lookups using SPL or the Lookup Editor. You can learn more about lookups from the Splunk documentation.

NEW QUESTION 233
- (Exam Topic 2)
The stats command will create a _____ by default.

A. Table
B. Report
C. Pie chart

Answer: A

NEW QUESTION 236
- (Exam Topic 2)
A user wants to create a new field alias for a field that appears in two sourcetypes. How many field aliases need to be created?

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

Answer: B

NEW QUESTION 238
- (Exam Topic 2)
Use the dedup command to _____.

A. Rename a field in the index
B. remove duplicate values

C. provide an additional alias for the field that can
D. be used in the search criteria

Answer: B

NEW QUESTION 243
- (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 245
- (Exam Topic 2)
The eval command allows you to do which of the following? (Choose all that apply.)

A. Format values
B. Convert values
C. Perform calculations
D. Use conditional statements

Answer: ABCD

NEW QUESTION 246
- (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 248
- (Exam Topic 2)
When used with the timechart command, which value of the limit argument returns all values?

A. limit=*
B. limit=all
C. limit=none
D. limit=0

Answer: D

Explanation:
The correct answer is D. limit=0. This is because the limit argument specifies the maximum number of series to display in the chart. If you set limit=0, no series filtering occurs and all values are returned. You can learn more about the limit argument and how it works with the agg argument from the Splunk documentation1.
The other options are incorrect because they are not valid values for the limit argument. The limit argument expects an integer value, not a string or a wildcard.
You can learn more about the syntax and usage of the timechart command from the Splunk documentation23.

NEW QUESTION 253
- (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 255
- (Exam Topic 2)
_____ datasets can be added to root dataset to narrow down the search

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

Answer: D

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

NEW QUESTION 256
- (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 257
- (Exam Topic 2)
A macro has another macro nested within it, and this inner macro requires an argument. How can the user pass this argument into the SPL?

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

Answer: D

Explanation:
The correct answer is D. An argument can be passed to the inner macro by nesting parentheses.
A search macro is a way to reuse a piece of SPL code in different searches. A search macro can take arguments, which are variables that can be replaced by different values when the macro is called. A search macro can also contain another search macro within it, which is called a nested macro. A nested macro can also take arguments, which can be passed from the outer macro or directly from the search string.
To pass an argument to the inner macro, you need to use parentheses to enclose the argument value and separate it from the outer macro argument. For example, if you have a search macro named outer_macro (1) that contains another search macro named inner_macro (2), and both macros take one argument each, you can pass an argument to the inner macro by using the following syntax:
outer_macro (argument1, inner_macro (argument2))
This will replace the argument1 and argument2 with the values you provide in the search string. For example, if you want to pass “foo” as the argument1 and “bar” as the argument2, you can write:
outer_macro ("foo", inner_macro ("bar"))
This will expand the macros with the corresponding arguments and run the SPL code contained in them. References:
- Search macro examples
- Use search macros in searches

NEW QUESTION 262
- (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 263
- (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 268
- (Exam Topic 2)
If there are fields in the data with values that are " " or empty but not null, which of the following would add a value?

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

Answer: D

Explanation:
The correct answer is D. | eval notNULL = “” fillnull value=0 notNULL

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

NEW QUESTION 272
- (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 273
- (Exam Topic 2)
Which of the following describes the I transaction command?

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

Answer: C

Explanation:

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

NEW QUESTION 278
- (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 280
- (Exam Topic 2)
Which of the following statements would help a user choose between the transaction and stats commands?

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

Answer: C

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchReference/Transaction
One of the statements that would help a user choose between the transaction and stats commands is that there is a 1000 event limitation with the transaction command3. The transaction command is used to group events that share a common value for one or more fields into transactions3. The transaction command has a default limit of 1000 events per transaction, which means that it will not group more than 1000 events into a single transaction3. This limit can be changed by using the maxevents parameter, but it can affect the performance and memory usage of Splunk3. Therefore, option C is correct, while options A, B and D are incorrect because they are not statements that would help a user choose between the transaction and stats commands.

NEW QUESTION 285
- (Exam Topic 2)
How is a Search Workflow Action configured to run at the same time range as the original search?

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

Answer: C

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

NEW QUESTION 290
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SPLK-1002 Exam with Our Prep Materials Via below:

https://www.certleader.com/SPLK-1002-dumps.html