Number: SPLK-1002
Passing Score: 800
Time Limit: 120
File Version: 14.0

Exam Code: SPLK-1002
Exam Name: Splunk Core Certified Power User

Exam A

QUESTION 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

Correct Answer: B
Section:
Explanation:
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.

QUESTION 2
Which of the following statements describes this search?
sourcetype=access_combined I transaction JSESSIONID | timechart avg (duration)

A. This is a valid search and will display a timechart of the average duration, of each transaction event.
B. This is a valid search and will display a stats table showing the maximum pause among transactions.
C. No results will be returned because the transaction command must include the startswith and endswith options.
D. No results will be returned because the transaction command must be the last command used in the search pipeline.

Correct Answer: A
Section:
Explanation:
This search uses the transaction command to group events that share a common value for JSESSIONID into transactions1.The transaction command assigns a duration field to each transaction, which is the difference between the latest and earliest timestamps of the events in the transaction1.The search then uses the timechart command to create a time-series chart of the average duration of each transaction1. Therefore, option A is correct because it describes the search accurately. Option B is incorrect because the search does not use the stats command or the pause field.Option C is incorrect because the transaction command does not require the startswith and endswith options, although they can be used to specify how to identify the beginning and end of a transaction1.Option D is incorrect because the transaction command does not have to be the last command in the search pipeline, although it is often used near the end of a search1.

QUESTION 3
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

Correct Answer: B

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

QUESTION 4
Which method in the Field Extractor would extract the port number from the following event? |
10/20/2022 - 125.24.20.1 ++++ port 54 - user: admin <web error>

A. Delimiter
B. rex command
C. The Field Extractor tool cannot extract regular expressions.
D. Regular expression

Correct Answer: B
Section:
Explanation:
The rex command allows you to extract fields from events using regular expressions. You can use the rex command to specify a named group that matches the port number in the event. For example:
rex '\+\+\+\+port (?\d+)'
This will create a field called port with the value 54 for the event.
The delimiter method is not suitable for this event because there is no consistent delimiter between the fields. The regular expression method is not a valid option for the Field Extractor tool. The Field Extractor tool can extract regular expressions, but it is not a method by itself.

QUESTION 5
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)'

Correct Answer: C
Section:
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.

QUESTION 6
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

Correct Answer: C
Section:
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.

QUESTION 7
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)

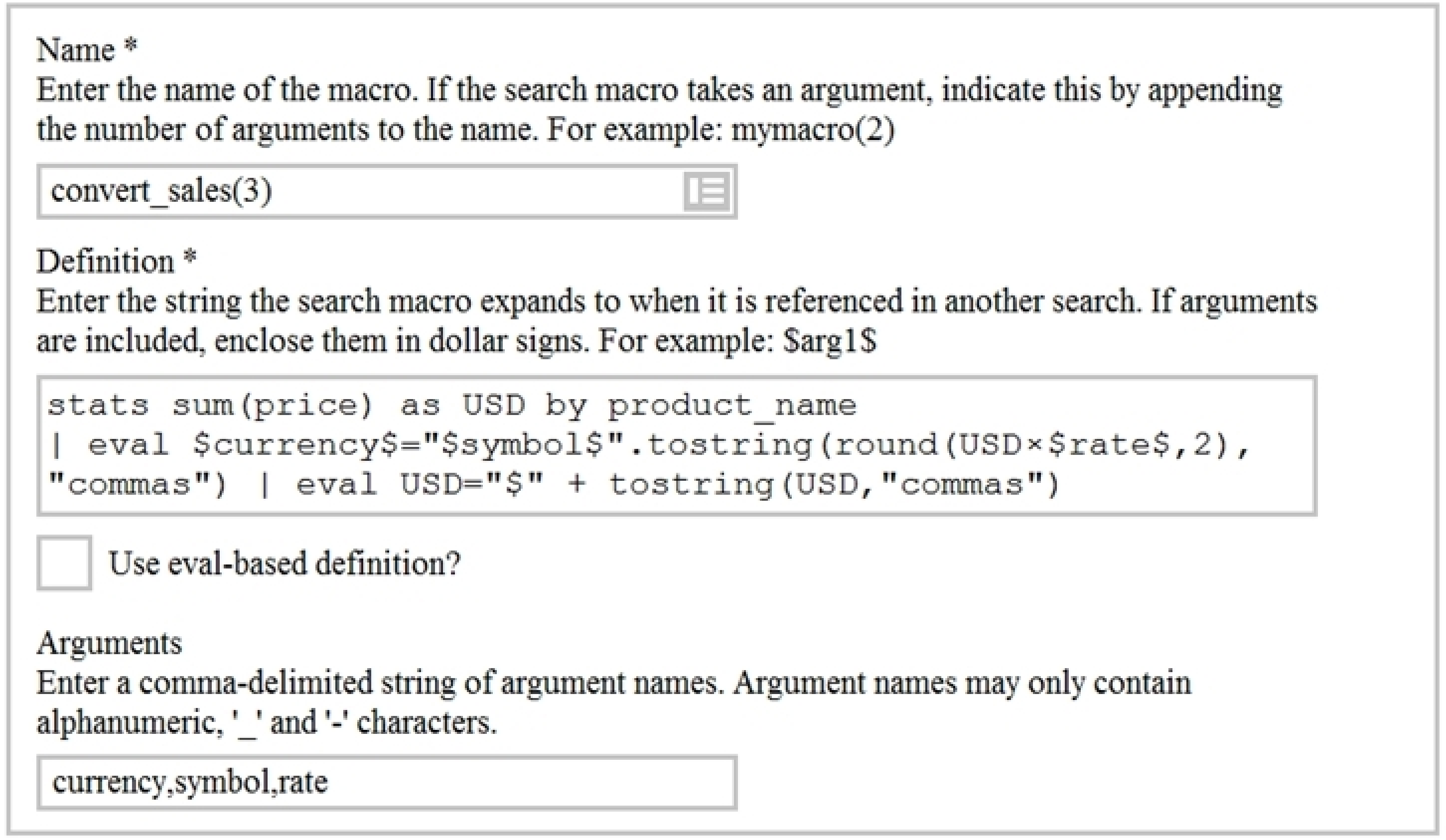
Correct Answer: C
Section:
Explanation:
The correct answer is C. 'weekly_sales (3.99, 10)'. This is because search macros accept arguments without quotation marks or dollar signs, and the number of arguments must match the number of parameters defined in the macro. The other options are incorrect because 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.

QUESTION 8
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

Correct Answer: B
Section:
Explanation:
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.

QUESTION 9
Based on the macro definition shown below, what is the correct way to execute the macro in a search string?



Name *
Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to the name. For example: mymacro(2)

convert_sales(3)

Definition *
Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: $arg1$

```
stats sum(price) as USD by product_name
| eval $currency$="$symbol$".tostring(round(USD×$rate$,2),
"commas") | eval USD="$" + tostring(USD,"commas")
```

Use eval-based definition?

Arguments
Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.

currency,symbol,rate

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

Correct Answer: B
Section:
Explanation:
The correct way to execute the macro in a search string is to use the formatmacro_name($arg1$, $arg2$, ...)where$arg1$,$arg2$, etc. are the arguments for the macro. In this case, the macro name isconvert_salesand it takes three arguments:currency,symbol, andrate. The arguments are enclosed in dollar signs and separated by commas. Therefore, the correct way to execute the macro isconvert_sales($euro$, $$, .79).

QUESTION 10
Which of the following statements describe data model acceleration? (select all that apply)

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

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

QUESTION 11
A user wants to convert numeric field values to strings and also to sort on those values.
Which command should be used first, the eval or the sort?

A. It doesn't matter whether eval or sort is used first.
B. Convert the numeric to a string with eval first, then sort.
C. Use sort first, then convert the numeric to a string with eval.
D. You cannot use the sort command and the eval command on the same field.

Correct Answer: C
Section:
Explanation:
The eval command is used to create new fields or modify existing fields based on an expression2.The sort command is used to sort the results by one or more fields in ascending or descending order2.If you want to convert numeric field values to strings and also sort on those values, you should use the sort command first, then use the eval command to convert the values to strings2. This way, the sort command will use the original numeric values for sorting, rather than the converted string values which may not sort correctly. Therefore, option C is correct, while options A, B and D are incorrect.

QUESTION 12
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.

Correct Answer: C, D
Section:
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.

QUESTION 13
Which of the following data model are included In the Splunk Common Information Model (CIM) add-on? (select all that apply)

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

Correct Answer: A, B, C
Section:
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 several data models that cover various domains such as Alerts, Email, Database, Network Traffic, Web and more3. Therefore, options A, B and C are correct because they are names of some of the data models included in the CIM add-on. Option D is incorrect because User permissions is not a name of a data model in the CIM add-on.

QUESTION 14
Which one of the following statements about the search command is true?

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

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

QUESTION 15
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

Correct Answer: B, C
Section:
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.

QUESTION 16
Which of the following file formats can be extracted using a delimiter field extraction?

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

Correct Answer: A
Section:
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.

QUESTION 17
Which of the following statements describes macros?

A. A macro is a reusable search string that must contain the full search.
B. A macro is a reusable search string that must have a fixed time range.
C. A macro Is a reusable search string that may have a flexible time range.
D. A macro Is a reusable search string that must contain only a portion of the search.

Correct Answer: C
Section:
Explanation:
A macro is a reusable search string that can contain any part of a search, such as search terms, commands, arguments, etc. A macro can have a flexible time range that can be specified when the macro is executed. A macro can also have arguments that can be passed to the macro when it is executed. A macro can be created by using the Settings menu or by editing the macros.conf file. A macro does not have to contain the full search, but only the part that needs to be reused. A macro does not have to have a fixed time range, but can use a relative or absolute time range modifier. A macro does not have to contain only a portion of the search, but can contain multiple parts of the search.

QUESTION 18
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

Correct Answer: C
Section:
Explanation:
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.

QUESTION 19
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.

Correct Answer: B, C, D
Section:
Explanation:
The commandsourcetype=access_combined | transaction JSESSIONIDdoes three things:
It filters the events by the sourcetypeaccess_combined, which is a predefined sourcetype for Apache web server logs.
It groups the events by the fieldJSESSIONID, which is a unique identifier for each user session.
It creates a single event from each group of events that share the sameJSESSIONIDvalue. This single event will have some additional fields created by the transaction command, such asduration,eventcount, andstartime.
Therefore, the statements B, C, and D are true.

QUESTION 20
Which of the following can be used with the eval command tostring function (select all that apply)

A. ''hex''
B. ''commas''
C. ''Decimal''
D. ''duration''

Correct Answer: A, B, D
Section:
Explanation:
https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/ConversionFunctions#tostring.28X.2CY.29
The tostring function in the eval command converts a numeric value to a string value. It can take an optional second argument that specifies the format of the string value. Some of the possible formats are:
hex: converts the numeric value to a hexadecimal string.
commas: adds commas to separate thousands in the numeric value.
duration: converts the numeric value to a human-readable duration string, such as ''2h 3m 4s''.
Therefore, the formats A, B, and D can be used with the tostring function.

QUESTION 21
Which of the following statements about tags is true?

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

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

QUESTION 22
Which of the following statements about data models and pivot are true? (select all that apply)

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

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

QUESTION 23
When using the Field Extractor (FX), which of the following delimiters will work? (select all that apply)

A. Tabs
B. Pipes
C. Colons
D. Spaces

Correct Answer: A, B, D
Section:
Explanation:
https://community.splunk.com/t5/Splunk-Search/Field-Extraction-Separate-on-Colon/m-p/29751
The Field Extractor (FX) is a tool that helps you extract fields from your data using delimiters or regular expressions. Delimiters are characters or strings that separate fields in your data. Some of the delimiters that will work with FX are:
Tabs: horizontal spaces that align text in columns.
Pipes: vertical bars that often indicate logical OR operations.
Spaces: blank characters that separate words or symbols.
Therefore, the delimiters A, B, and D will work with FX.

QUESTION 24
Which of the following describes the Splunk Common Information Model (CIM) add-on?

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

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

QUESTION 25
What does the transaction command do?

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

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

QUESTION 26

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

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

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

QUESTION 27
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.

Correct Answer: B
Section:
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.

QUESTION 28
When should you use the transaction command instead of the scats command?

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

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

QUESTION 29
Which of the following statements describes field aliases?

A. Field alias names replace the original field name.
B. Field aliases can be used in lookup file definitions.
C. Field aliases only normalize data across sources and sourcetypes.
D. Field alias names are not case sensitive when used as part of a search.

Correct Answer: B
Section:
Explanation:
Field aliases are alternative names for fields in Splunk. Field aliases can be used to normalize data across different sources and sourcetypes that have different field names for the same concept. For example, you can create a field alias for src_ip that maps to clientip, source_address, or any other field name that represents the source IP address in different sourcetypes. Field aliases can also be used in lookup file definitions to map fields in your data to fields in the lookup file. For example, you can use a field alias for src_ip to map it to ip_address in a lookup file that contains geolocation information for IP addresses. Field alias names do not replace the original field name, but rather create a copy of the field with a different name. Field alias names are case sensitive when used as part of a search, meaning that src_ip and SRC_IP are different fields.

QUESTION 30
What is the correct way to name a macro with two arguments?

A. us_sales2
B. us_sales(1,2)
C. us_sale,2
D. us_sales(2)

Correct Answer: D
Section:

QUESTION 31
When using a field value variable with a Workflow Action, which punctuation mark will escape the data

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

Correct Answer: B
Section:
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.

QUESTION 32
__________ datasets can be added to root dataset to narrow down the search

A. parent
B. extracted

C. event
D. child

Correct Answer: D
Section:
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.

QUESTION 33
Which function should you use with the transaction command to set the maximum total time between the earliest and latest events returned?

A. maxpause
B. endswith
C. maxduration
D. maxspan

Correct Answer: D
Section:
Explanation:
The maxspan function of the transaction command allows you to set the maximum total time between the earliest and latest events returned. The maxspan function is an argument that can be used with the transaction command to specify the start and end constraints for the transactions. The maxspan function takes a time modifier as its value, such as 30s, 5m, 1h, etc. The maxspan function sets the maximum time span between the first and last events in a transaction. If the time span between the first and last events exceeds the maxspan value, the transaction will be split into multiple transactions.

QUESTION 34
The eval command 'if' function requires the following three arguments (in order):

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

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

QUESTION 35
Which search would limit an 'alert' tag to the 'host' field?

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

D. tag::host=alert

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

QUESTION 36
The transaction command allows you to ___________ events across multiple sources

A. duplicate
B. correlate
C. persist
D. tag

Correct Answer: B
Section:
Explanation:
The transaction command allows you to correlate events across multiple sources. The transaction command is a search command that allows you to group events into transactions based on some common characteristics, such as fields, time, or both. A transaction is a group of events that share one or more fields that relate them to each other. A transaction can span across multiple sources or sourcetypes that have different formats or structures of data. The transaction command can help you correlate events across multiple sources by using the common fields as the basis for grouping. The transaction command can also create some additional fields for each transaction, such as duration, eventcount, startime, etc.

QUESTION 37
which of the following commands are used when creating visualizations(select all that apply.)

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

Correct Answer: A, C, D
Section:
Explanation:
The following commands are used when creating visualizations: geom, geostats, and iplocation. Visualizations are graphical representations of data that show trends, patterns, or comparisons. Visualizations can have different types, such as charts, tables, maps, etc. Visualizations can be created by using various commands that transform the data into a suitable format for the visualization type. Some of the commands that are used when creating visualizations are:
geom: This command is used to create choropleth maps that show geographic regions with different colors based on some metric. The geom command takes a KMZ file as an argument that defines the geographic regions and their boundaries. The geom command also takes a field name as an argument that specifies the metric to use for coloring the regions.
geostats: This command is used to create cluster maps that show groups of events with different sizes and colors based on some metric. The geostats command takes a latitude and longitude field as arguments that specify the location of the events. The geostats command also takes a statistical function as an argument that specifies the metric to use for sizing and coloring the clusters.
iplocation: This command is used to create location-based visualizations that show events with different attributes based on their IP addresses. The iplocation command takes an IP address field as an argument and adds some additional fields to the events, such as Country, City, Latitude, Longitude, etc. The iplocation command can be used with other commands such as geom or geostats to create maps based on IP addresses.

QUESTION 38
For choropleth maps,splunk ships with the following KMZ files (select all that apply)

A. States of the United States
B. States and provinces of the united states and Canada
C. Countries of the European Union
D. Countries of the World

Correct Answer: A, D
Section:
Explanation:
Splunk ships with the following KMZ files for choropleth maps: States of the United States and Countries of the World. A KMZ file is a compressed file that contains a KML file and other resources. A KML file is an XML file that defines geographic features and their properties. A KMZ file can be used to create choropleth maps in Splunk by using the geom command. A choropleth map is a type of map that shows geographic regions with different colors based on some metric. Splunk ships with two KMZ files that define the geographic regions for choropleth maps:
States of the United States: This KMZ file defines the 50 states of the United States and their boundaries. The name of this KMZ file is us_states.kmz and it is located in the $SPLUNK_HOME/etc/apps/maps/appserver/static/geo directory.
Countries of the World: This KMZ file defines the countries of the world and their boundaries. The name of this KMZ file is world_countries.kmz and it is located in the $SPLUNK_HOME/etc/apps/maps/appserver/static/geo directory.
Splunk does not ship with KMZ files for States and provinces of the United States and Canada or Countries of the European Union. However, you can create your own KMZ files or download them from external sources and use them in Splunk.

QUESTION 39
What does the following search do?

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


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

Correct Answer: B
Section:
Explanation:
The search string below creates a table of the total count of mysterymeat corndogs split by user.
| stats count by user | where corndog=mysterymeat
The search string does the following:
It uses the stats command to calculate the count of events for each value of the user field. The stats command creates a table with two columns: user and count.
It uses the where command to filter the results by the value of the corndog field. The where command only keeps the rows where corndog equals mysterymeat.
Therefore, the search string creates a table of the total count of mysterymeat corndogs split by user.

QUESTION 40
Which of the following statements describes Search workflow actions?

A. By default. Search workflow actions will run as a real-time search.
B. Search workflow actions can be configured as scheduled searches,
C. The user can define the time range of the search when created the workflow action.

D. Search workflow actions cannot be configured with a search string that includes the transaction command

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

QUESTION 41
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.

Correct Answer: D
Section:
Explanation:
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.

QUESTION 42
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

Correct Answer: D
Section:
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.

QUESTION 43
Data model are composed of one or more of which of the following datasets? (select all that apply.)

A. Events datasets
B. Search datasets
C. Transaction datasets

D. Any child of event, transaction, and search datasets

Correct Answer: A, B, C
Section:
Explanation:
Data models are collections of datasets that represent your data in a structured and hierarchical way. Data models define how your data is organized into objects and fields. Data models can be composed of one or more of the following datasets:
Events datasets: These are the base datasets that represent raw events in Splunk. Events datasets can be filtered by constraints, such as search terms, sourcetypes, indexes, etc.
Search datasets: These are derived datasets that represent the results of a search on events or other datasets. Search datasets can use any search command, such as stats, eval, rex, etc., to transform the data.
Transaction datasets: These are derived datasets that represent groups of events that are related by fields, time, or both. Transaction datasets can use the transaction command or event types with transactiontype=true to create transactions.

QUESTION 44
Which are valid ways to create an event type? (select all that apply)

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

Correct Answer: C, D
Section:
Explanation:
Event types are custom categories of events that are based on search criteria. Event types can be used to label events with meaningful names, such as error, success, login, logout, etc. Event types can also be used to create transactions, alerts, reports, dashboards, etc. Event types can be created in two ways:
By going to the Settings menu and clicking Event Types > New. This will open a form where you can enter the name, description, search string, app context, and tags for the event type.
By selecting an event in search results and clicking Event Actions > Build Event Type. This will open a dialog box where you can enter the name and description for the event type. The search string will be automatically populated based on the selected event.
Event types cannot be created by using the searchtypes command in the search bar, as this command does not exist in Splunk. Event types can also be created by editing the event_type stanza in the transforms.conf file, not the props.conf file.

QUESTION 45
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 bystate.
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

Correct Answer: B
Section:
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.

QUESTION 46
What is the relationship between data models and pivots?

A. Data models provide the datasets for pivots.
B. Pivots and data models have no relationship.
C. Pivots and data models are the same thing.
D. Pivots provide the datasets for data models.

Correct Answer: A
Section:
Explanation:
The relationship between data models and pivots is that data models provide the datasets for pivots. Data models are collections of datasets that represent your data in a structured and hierarchical way. Data models define how your data is organized into objects and fields. Pivots are user interfaces that allow you to create data visualizations that present different aspects of a data model. Pivots let you select options from menus and forms to create charts, tables, maps, etc., without writing any SPL code. Pivots use datasets from data models as their source of data. Pivots and data models are not the same thing, as pivots are tools for visualizing data models. Pivots do not provide datasets for data models, but rather use them as inputs.
Therefore, only statement A is true about the relationship between data models and pivots.

QUESTION 47
What are the two parts of a root event dataset?

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

Correct Answer: C
Section:
Explanation:
A root event dataset is the base dataset for a data model that defines the source or sources of the data and the constraints and fields that apply to the data1.A root event dataset has two parts: constraints and fields1.Constraints are filters that limit the data to a specific index, source, sourcetype, host or search string1.Fields are the attributes that describe the data and can be extracted, calculated or looked up1. Therefore, option C is correct, while options A, B and D are incorrect.

QUESTION 48
In which of the following scenarios is an event type more effective than a saved search?

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

Correct Answer: C
Section:
Explanation:
An event type is a way to categorize events based on a search string that matches the events2.You can use event types to simplify your searches by replacing long or complex search strings with short and simple event type names2.An event type is more effective than a saved search when the search string needs to be used in future searches because it allows you to reuse the search string without having to remember or type it again2.

Therefore, option C is correct, while options A, B and D are incorrect because they are not scenarios where an event type is more effective than a saved search.

QUESTION 49
How does a user display a chart in stack mode?

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

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

QUESTION 50
Which of the following statements about event types is true? (select all that apply)

A. Event types can be tagged.
B. Event types must include a time range,
C. Event types categorize events based on a search.
D. Event types can be a useful method for capturing and sharing knowledge.

Correct Answer: A, C, D
Section:
Explanation:
As mentioned before, an event type is a way to categorize events based on a search string that matches the events2.Event types can be tagged, which means that you can apply descriptive labels to event types and use them in your searches2. Therefore, option A is correct.Event types categorize events based on a search string, which means that you can define an event type by specifying a search string that matches the events you want to include in the event type2. Therefore, option C is correct.Event types can be a useful method for capturing and sharing knowledge, which means that you can use event types to organize your data into meaningful categories and share them with other users in your organization2. Therefore, option D is correct.Event types do not have to include a time range, which means that you can create an event type without specifying a time range for the events2. Therefore, option B is incorrect.

QUESTION 51
In what order arc the following knowledge objects/configurations applied?

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

Correct Answer: B
Section:
Explanation:
Knowledge objects are entities that you create to add knowledge to your data and make it easier to search and analyze2.Some examples of knowledge objects are field extractions, field aliases and lookups2.Field extractions are methods that extract fields from your raw data using various techniques such as regular expressions, delimiters or key-value pairs2.Field aliases are ways to assign alternative names to existing fields without changing the original field names or values2.Lookups are ways to enrich your data with additional information from external sources such as CSV files or databases2.The order in which these knowledge objects/configurations are applied is

as follows: field extractions, field aliases and then lookups2.This means that Splunk first extracts fields from your raw data, then applies any aliases to the extracted fields and then performs any lookups on the aliased fields2. Therefore, option B is correct, while options A, C and D are incorrect.

QUESTION 52
Which of the following knowledge objects represents the output of an eval expression?

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

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

QUESTION 53
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

Correct Answer: B
Section:
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.

QUESTION 54
Which of the following eval command function is valid?

A. Int ()
B. Count ( )
C. Print ()
D. Tostring ()

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

QUESTION 55
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.

Correct Answer: B, C
Section:
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.

QUESTION 56
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.

Correct Answer: A
Section:
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.

QUESTION 57
Which of the following statements describes POST workflow actions?

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

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

QUESTION 58
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

Correct Answer: A, C
Section:
Explanation:
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 macros 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.

QUESTION 59
Which of the following workflow actions can be executed from search results? (select all that apply)

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

Correct Answer: A, B, D
Section:
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.

QUESTION 60
Which of the following is the correct way to use the data model command to search field in the data model within the web dataset?

A. | datamodel web search | filed web *
B. | Search datamodel web web | filed web*
C. | datamodel web web field | search web*
D. Datamodel=web | search web | filed web*

Correct Answer: A
Section:
Explanation:
The data model command allows you to run searches on data models that have been accelerated1.The syntax for using the data model command is| datamodel <model_name> <dataset_name> [search <search_string>]1. Therefore, option A is the correct way to use the data model command to search fields in the data model within the web dataset. Options B and C are incorrect because they do not follow the syntax for the data model command. Option D is incorrect because it does not use the data model command at all.

QUESTION 61
When a search returns __________, you can view the results as a list.

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

Correct Answer: C
Section:

QUESTION 62
The timechart command buckets data in time intervals depending on:

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

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

QUESTION 63
There are several ways to access the field extractor. Which option automatically identifies data type, source type, and sample event?

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

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

QUESTION 64
Which statement is true?

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

Correct Answer: C
Section:

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

QUESTION 65
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.

Correct Answer: C
Section:

QUESTION 66
When using | timchart by host, which filed is representted in the x-axis?

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

Correct Answer: A
Section:

QUESTION 67
Which of the following statements describes POST workflow actions?

A. Configuration of a POST workflow action includes choosing a sourcetype.
B. POST workflow actions can be configured to send email to the URI location.
C. By default, POST workflow action are shown in both the event and field menus.
D. POST workflow actions can be configured to send POST arguments to the URI location.

Correct Answer: D
Section:

QUESTION 68
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.

Correct Answer: D
Section:

QUESTION 69
Which workflow action method can be used the action type is set to link?

A. GET
B. PUT
C. Search
D. UPDATE

Correct Answer: A
Section:
Explanation:
https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/SetupaGETworkflowaction
Define a GET workflow action
Steps
Navigate toSettings > Fields > Workflow Actions.
ClickNewto open up a new workflow action form.
Define aLabelfor the action.
TheLabelfield 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.
UseApply only to the following fieldsto 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.
UseApply only to the following event typesto 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.
ForShow action indetermine whether you want the action to appear in theEvent menu, theFields menus, orBoth.
SetAction typetolink.
InURIprovide a URI for the location of the external resource that you want to send your field values to.
Similar to theLabelsetting, 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 automaticallyURL encodedduring transmission. This means you can include values that have spaces between words or punctuation characters.
UnderOpen link in, determine whether the workflow action displays in the current window or if it opens the link in a new window.
Set theLink methodtoget.
ClickSaveto save your workflow action definition.

QUESTION 70
When using | timechart by host, which field is represented in the x-axis?

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

Correct Answer: D
Section:

QUESTION 71
Clicking a SEGMENT on a chart, ________.

A. drills down for that value
B. highlights the field value across the chart

C. adds the highlighted value to the search criteria

Correct Answer: C
Section:

QUESTION 72
Use this command to use lookup fields in a search and see the lookup fields in the field sidebar.

A. inputlookup
B. lookup

Correct Answer: B
Section:

QUESTION 73
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

Correct Answer: D
Section:

QUESTION 74
Which is not a comparison operator in Splunk

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

Correct Answer: E
Section:
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

QUESTION 75
Which of the following is NOT a stats function:

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

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

QUESTION 76
If a search returns _____________ it can be viewed as a chart.

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

Correct Answer: B
Section:
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.

QUESTION 77
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

Correct Answer: C
Section:
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.

QUESTION 78
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

Correct Answer: C
Section:

QUESTION 79
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

Correct Answer: A, B, C, D
Section:

QUESTION 80
When using the timechart command, how can a user group the events into buckets based on time?

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

Correct Answer: A
Section:

QUESTION 81
Which type of visualization shows relationships between discrete values in three dimensions?

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

Correct Answer: C
Section:
Explanation:
https://docs.splunk.com/Documentation/DashApp/0.9.0/DashApp/chartsBub

QUESTION 82
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.

Correct Answer: A
Section:

QUESTION 83

What information must be included when using the datamodel command?

A. status field
B. Multiple indexes
C. Data model field name.
D. Data model dataset name.

Correct Answer: D
Section:

QUESTION 84
A data model can consist of what three types of datasets?

A. Pivot, searches, and events.
B. Pivot, events, and transactions.
C. Searches, transactions, and pivot.
D. Events, searches, and transactions.

Correct Answer: D
Section:

QUESTION 85
When is a GET workflow action needed?

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

Correct Answer: B
Section:

QUESTION 86
Which command can include both an over and a by clause to divide results into sub-groupings?

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

Correct Answer: A
Section:

QUESTION 87
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.

Correct Answer: B
Section:

QUESTION 88
In the following eval statement, what is the value of description if the status is 503? index=main | eval description=case(status==200, 'OK', status==404, 'Not found', status==500, 'Internal Server Error')

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

Correct Answer: A
Section:
Explanation:
https://docs.splunk.com/Documentation/Splunk/8.1.1/SearchReference/ConditionalFunctions

QUESTION 89
In which Settings section are macros defined?

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

Correct Answer: C
Section:

QUESTION 90
Which of the following statements describes calculated fields?

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

Correct Answer: B
Section:

QUESTION 91
Which of the following is one of the pre-configured data models included in the Splunk Common Information Model (CIM) add-on?

A. Access

B. Accounting
C. Authorization
D. Authentication

Correct Answer: D
Section:

QUESTION 92
What happens when a user edits the regular expression (regex) field extraction generated in the Field Extractor (FX)?

A. There is a limit to the number of fields that can be extracted.
B. The user is unable to preview the extractions.
C. The extraction is added at index time.
D. The user is unable to return to the automatic field extraction workflow.

Correct Answer: A
Section:

QUESTION 93
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

Correct Answer: B
Section:

QUESTION 94
Data models are composed of one or more of which of the following datasets? (select all that apply)

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

Correct Answer: A, B, C
Section:
Explanation:
Data model datasets have a hierarchical relationship with each other, meaning they have parent-child relationships. Data models can contain multiple dataset hierarchies. There are three types of dataset hierarchies: event, search, and transaction.
https://docs.splunk.com/Splexicon:Datamodeldataset

QUESTION 95

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)

Correct Answer: C
Section:
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].

QUESTION 96
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

Correct Answer: A, C
Section:
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 ('').

QUESTION 97
Which of the following statements describes the use of the Field Extractor (FX)?

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

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

QUESTION 98
Which of the following eval command functions is valid?

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

D. tostring()

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

QUESTION 99
When creating a data model, which root dataset requires at least one constraint?

A. Root transaction dataset
B. Root event dataset
C. Root child dataset
D. Root search dataset

Correct Answer: B
Section:
Explanation:
The correct answer is B. Root event dataset. This is because root event datasets are defined by a constraint that filters out events that are not relevant to the dataset. A constraint for a root event dataset is a simple search that returns a fairly wide range of data, such as sourcetype=access_combined. Without a constraint, a root event dataset would include all the events in the index, which is not useful for data modeling. You can learn more about how to design data models and add root event datasets from the Splunk documentation1. The other options are incorrect because root transaction datasets and root search datasets have different ways of defining their datasets, such as transaction definitions or complex searches, and root child datasets are not a valid type of root dataset.

QUESTION 100
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.

Correct Answer: C
Section:
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.

QUESTION 101
What type of command is eval?

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

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

QUESTION 102
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.

Correct Answer: C
Section:
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.

QUESTION 103
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

Correct Answer: D
Section:
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.

QUESTION 104
Which field extraction method should be selected for comma-separated data?

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

Correct Answer: B

Section:
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
.

QUESTION 105
What approach is recommended when using the Splunk Common Information Model (CIM) add-on to normalize data?

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

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

QUESTION 106
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

Correct Answer: B
Section:
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.

QUESTION 107
For the following search, which field populates the x-axis?
index=security sourcetype=linux secure | timechart count by action

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

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

QUESTION 108
In the Field Extractor, when would the regular expression method be used?

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

Correct Answer: C
Section:
Explanation:
The correct answer is C. When events contain unstructured data.
The regular expression method works best with unstructured event data, such as log files or text messages, where the fields are not separated by a common delimiter, such as a comma or space1. You select a sample event and highlight one or more fields to extract from that event, and the field extractor generates a regular expression that matches similar events in your dataset and extracts the fields from them1. The regular expression method provides several tools for testing and refining the accuracy of the regular expression. It also allows you to manually edit the regular expression1.
The delimiters method is designed for structured event data: data from files with headers, where all of the fields in the events are separated by a common delimiter, such as a comma or space1. You select a sample event, identify the delimiter, and then rename the fields that the field extractor finds1. This method is simpler and faster than the regular expression method, but it may not work well with complex or irregular data formats1.
1: Build field extractions with the field extractor - Splunk Documentation

QUESTION 109
These users can create global knowledge objects. (Select all that apply.)

A. users
B. power users
C. administrators

Correct Answer: B, C
Section:

QUESTION 110
This is what Splunk uses to categorize the data that is being indexed.

A. sourcetype
B. index
C. source
D. host

Correct Answer: A
Section:

QUESTION 111
This is what Splunk uses to categorize the data that is being indexed.

A. Host
B. Sourcetype
C. Index
D. Source

Correct Answer: B
Section:

QUESTION 112
By default search results are not returned in _________ order.

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

Correct Answer: A, D
Section:

QUESTION 113
The stats command will create a ______________ by default.

A. Table
B. Report
C. Pie chart

Correct Answer: A
Section:

QUESTION 114
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

Correct Answer: A
Section:

QUESTION 115
What are search macros?

A. Lookup definitions in lookup tables.
B. Reusable pieces of search processing language.
C. A method to normalize fields.
D. Categories of search results.

Correct Answer: B
Section:
Explanation:
The correct answer is B. Reusable pieces of search processing language.
The explanation is as follows:
Search macros are knowledge objects that allow you to insert chunks of SPL into other searches12.
Search macros can be any part of a search, such as an eval statement or a search term, and do not need to be a complete command12.
You can also specify whether the macro field takes any arguments and define validation expressions for them12.
Search macros can help you make your SPL searches shorter and easier to understand3.
To use a search macro in a search string, you need to put a backtick character () before and after the macro name[^1^][1]. For example, mymacro`.

QUESTION 116
Which of the following options will define the first event in a transaction?

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

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

QUESTION 117
Consider the following search:
index=web sourcetype=access_combined
The log shows several events that share the same JSESSIONID value (SD470K92802F117). View the events as a group.
From the following list, which search groups events by JSESSIONID?

A. index=web sourcetype=access_combined | highlight JSESSIONID | search SD470K92802F117
B. index=web sourcetype=access_combined | transaction JSESSIONID | search SD470K92802F117
C. index=web sourcetype=access_combined SD470K92802F117 | table JSESSIONID
D. index=web sourcetype=access_combined JSESSIONID <SD470K92802F117>

Correct Answer: B
Section:
Explanation:
To group events by JSESSIONID, the correct search is index=web sourcetype=access_combined | transaction JSESSIONID | search SD470K92802F117 (Option B). The transaction command groups events that share the same JSESSIONID value, allowing for the analysis of all events associated with a specific session as a single transaction. The subsequent search for SD470K92802F117 filters these grouped transactions to include only those related to the specified session ID.

QUESTION 118
When would transaction be used instead of stats?

A. To see results of a calculation.
B. To group events based on start/end values.
C. To have a faster and more efficient search.
D. To group events based on a single field value.

Correct Answer: B
Section:
Explanation:
The transaction command is used instead of stats to group events based on start/end values (Option B). This is particularly useful in scenarios where related events span across multiple log entries and need to be analyzed as a single transaction, such as user sessions or multi-step transaction processes.

QUESTION 119
Where are the descriptions of the data models that come with the Splunk Common Information Model (CIM) Add-on documented?

A. Datamodel command reference guide.
B. Pivot users manual.
C. Search and reporting user manual.
D. CIM Add-on manual.

Correct Answer: D
Section:
Explanation:
The CIM Add-on manual contains the descriptions of the data models that come with the Splunk Common Information Model (CIM) Add-on, as well as how to set up, use, and customize the add-on.
Reference
CIM Add-on manual
Splunk Common Information Model (CIM) | Splunkbase
Understand and use the Common Information Model Add-on - Splunk