Number: SPLK-1002
Passing Score: 800
Time Limit: 120
File Version: 4.0

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

Exam A

QUESTION 1
We can use the rename command to _____ (Select all that apply.)

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

Correct Answer: D
Section:

QUESTION 2
The limit attribute will_____.

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

Correct Answer: A
Section:

QUESTION 3
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 4

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 5
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 6
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 7
By default search results are not returned in _____ order.

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

Correct Answer: A, D
Section:

QUESTION 8

The stats command will create a _____ by default.

A. Table
B. Report
C. Pie chart

Correct Answer: A
Section:

QUESTION 9
This function of the stats command allows you to identify the number of values a field has.

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

Correct Answer: D
Section:

QUESTION 10
This function of the stats command allows you to return the sample standard deviation of a field.

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

Correct Answer: A
Section:

QUESTION 11
Which of the following commands will show the maximum bytes?

A. sourcetype=access_* | maximum totals by bytes
B. sourcetype=access_* | avg (bytes)
C. sourcetype=access_* | stats max(bytes)
D. sourcetype=access_* | max(bytes)

Correct Answer: C
Section:

QUESTION 12
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 13
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 14
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 15
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 16
_____ 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 17
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 18
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 19
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 20
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 21
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 22
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 23
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 24
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 25
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 26
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 27
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 28
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 29
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 30
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 31
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 32
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 33
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 34
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 35

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 36
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 37
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 38
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 39
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 40
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 41
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 42
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 43
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.

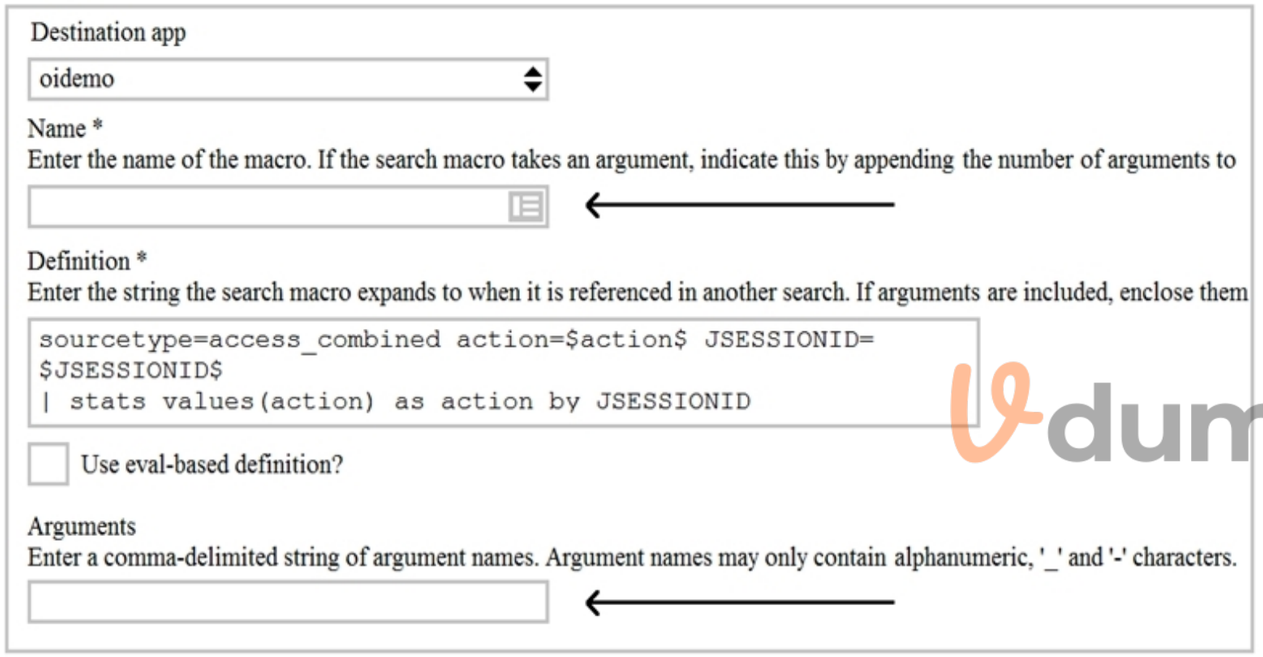
QUESTION 44
Which of the following statements describe the search below? (select all that apply)
Index=main I transaction clientip host maxspan=30s maxpause=5s

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

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

The search below groups events by two or more fields (clientip and host), creates transactions with start and end constraints (maxspan=30s and maxpause=5s), and calculates the duration of each transaction.
index=main | transaction clientip host maxspan=30s maxpause=5s
The search does the following:
It filters the events by the index main, which is a default index in Splunk that contains all data that is not sent to other indexes.
It uses the transaction command to group events into transactions based on two fields: clientip and host. The transaction command creates new events from groups of events that share the same clientip and host values.
It specifies the start and end constraints for the transactions using the maxspan and maxpause arguments. The maxspan argument sets the maximum time span between the first and last events in a transaction. The maxpause argument sets the maximum time span between any two consecutive events in a transaction. In this case, the maxspan is 30 seconds and the maxpause is 5 seconds, meaning that any transaction that has a longer time span or pause will be split into multiple transactions.
It creates some additional fields for each transaction, such as duration, eventcount, startime, etc. The duration field shows the time span between the first and last events in a transaction.

QUESTION 45
Given the macro definition below, what should be entered into the Name and Arguments fileds to correctly configured the macro?



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

Correct Answer: B
Section:
Explanation:
The macro definition below shows a macro that tracks user sessions based on two arguments: action and JSESSIONID.
sessiontracker(2)
The macro definition does the following:
It specifies the name of the macro as sessiontracker. This is the name that will be used to execute the macro in a search string.
It specifies the number of arguments for the macro as 2. This indicates that the macro takes two arguments when it is executed.
It specifies the code for the macro as index=main sourcetype=access_combined_wcookie action=$action$ JSESSIONID=$JSESSIONID$ | stats count by JSESSIONID. This is the search string that will be run when the macro is executed. The search string can contain any part of a search, such as search terms, commands, arguments, etc. The search string can also include variables for the arguments using dollar signs around them. In this case, action and JSESSIONID are variables for the arguments that will be replaced by their values when the macro is executed.

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

QUESTION 46
After manually editing; a regular expression (regex), which of the following statements is true?

A. Changes made manually can be reverted in the Field Extractor (FX) UI.
B. It is no longer possible to edit the field extraction in the Field Extractor (FX) UI.
C. It is not possible to manually edit a regular expression (regex) that was created using the Field Extractor (FX) UI.
D. The Field Extractor (FX) UI keeps its own version of the field extraction in addition to the one that was manually edited.

Correct Answer: B
Section:
Explanation:
After manually editing a regular expression (regex) that was created using the Field Extractor (FX) UI, it is no longer possible to edit the field extraction in the FX UI. The FX UI is a tool that helps you extract fields from your data using delimiters or regular expressions. The FX UI can generate a regex for you based on your selection of sample values or you can enter your own regex in the FX UI. However, if you edit the regex manually in the props.conf file, the FX UI will not be able to recognize the changes and will not let you edit the field extraction in the FX UI anymore. You will have to use the props.conf file to make any further changes to the field extraction. Changes made manually cannot be reverted in the FX UI, as the FX UI does not keep track of the changes made in the props.conf file. It is possible to manually edit a regex that was created using the FX UI, as long as you do it in the props.conf file.
Therefore, only statement B is true about manually editing a regex.

QUESTION 47
What does the fillnull command replace null values with, it the value argument is not specified?

A. 0
B. N/A
C. NaN
D. NULL

Correct Answer: A
Section:
Explanation:
The fillnull command is a search command that replaces null values with a specified value or 0 if no value is specified. Null values are values that are missing, empty, or undefined in Splunk. The fillnull command can replace null values for all fields or for specific fields. The fillnull command can take an optional argument called value that specifies the value to replace null values with. If no value argument is specified, the fillnull command will replace null values with 0 by default.

QUESTION 48
To identify all of the contributing events within a transaction that contains at least one REJECT event, which syntax is correct?

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

Correct Answer: B
Section:
Explanation:
The transaction command is used to group events that share a common value for one or more fields into transactions2.The transaction command assigns a transaction ID to each group of events and creates new fields such as duration, eventcount and eventlist for each transaction2.To identify all of the contributing events within a transaction that contains at least one REJECT event, you can use the following syntax:index=main | transaction

sessionid | search REJECT2.This search will first group the events by sessionid, then filter out the transactions that do not contain REJECT in any of their events2. Therefore, option B is correct, while options A, C and D are incorrect because they do not follow the correct syntax for using the transaction command or the search command.

QUESTION 49
Which of the following actions can the eval command perform?

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

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

QUESTION 50
Which of the following statements describe the Common Information Model (CIM)? (select all that apply)

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

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

QUESTION 51
Data model fields can be added using the Auto-Extracted method. Which of the following statements describe Auto-Extracted fields? (select all that apply)

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

Correct Answer: A, B, C, D
Section:
Explanation:
Data model fields are fields that describe the attributes of a dataset in a data model2.Data model fields can be added using various methods such as Auto-Extracted, Evaluated or Lookup2.Auto-Extracted fields are fields that

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

QUESTION 52
When creating a Search workflow action, which field is required?

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

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

QUESTION 53
Selected fields are displayed _____each event in the search results.

A. below
B. interesting fields
C. other fields
D. above

Correct Answer: A
Section:
Explanation:
Selected fields are fields that you choose to display in your search results by clicking on them in the Fields sidebar or by using the fields command2.Selected fields are displayed below each event in the search results, along with their values2. Therefore, option A is correct, while options B, C and D are incorrect because they are not places where selected fields are displayed.

QUESTION 54
A space is an implied _____ in a search string.

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

Correct Answer: B
Section:
Explanation:
A space is an implied AND in a search string, which means that it acts as a logical operator that returns events that match both terms on either side of the space2.For example,status=200 method=GETwill return events that

have both status=200 and method=GET2. Therefore, option B is correct, while options A, C and D are incorrect because they are not implied by a space in a search string.
Topic 2, Questions Set 2

QUESTION 55
Which of the following search control will not re-rerun the search? (Select all that apply.)

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

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

QUESTION 56
Highlighted search terms indicate _____ search results in Splunk.

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

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

QUESTION 57
When you mouse over and click to add a search term this (thesE. Boolean operator(s) is(arE. not implied. (Select all that apply).

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

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

QUESTION 58

The time range specified for a historical search defines the _____ .------questionable on ans

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

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

QUESTION 59
Using the export function, you can export search results as _____.(Select all that apply)

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

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

QUESTION 60
The fields sidebar does not show_____. (Select all that apply.)

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

Correct Answer: C
Section:
Explanation:
The fields sidebar is a panel that shows the fields that are present in your search results2.The fields sidebar does not show all extracted fields, which are fields that are extracted from your raw data using various methods such as regular expressions, delimiters or key-value pairs2.The fields sidebar only shows selected fields and interesting fields2.Selected fields are fields that you choose to display in your search results by clicking on them in the fields sidebar or by using the fields command2.Interesting fields are fields that appear in at least 20 percent of events or have high variability among values2. Therefore, option C is correct, while options A and B are incorrect because they are types of fields that the fields sidebar does show.

QUESTION 61
Splunk alerts can be based on search that run_____. (Select all that apply.)

A. in real-time
B. on a regular schedule

C. and have no matching events

Correct Answer: A, B
Section:
Explanation:
Splunk alerts can be based on searches that run in real-time or on a regular schedule3.An alert is a way to monitor your data and get notified when certain conditions are met3.You can create an alert by specifying a search and a triggering condition3.You can also specify how often you want to run the search and how you want to receive the alert notifications3.You can run the alert search in real-time, which means that it continuously monitors your data as it streams into Splunk3.Alternatively, you can run the alert search on a regular schedule, which means that it runs at fixed intervals such as every hour or every day3. Therefore, options A and B are correct, while option C is incorrect because it is not a way to run an alert search.

QUESTION 62
Which of the following about reports is/are true?

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

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

QUESTION 63
Select this in the fields sidebar to automatically pipe you search results to the rare command

A. events with this field
B. rare values
C. top values by time
D. top values

Correct Answer: B
Section:
Explanation:
The fields sidebar is a panel that shows the fields that are present in your search results2.The fields sidebar has two sections: selected fields and interesting fields2.Selected fields are fields that you choose to display in your search results by clicking on them in the fields sidebar or by using the fields command2.Interesting fields are fields that appear in at least 20 percent of events or have high variability among values2.For each field in the fields sidebar, you can select one of the following options: events with this field, rare values, top values by time or top values2.If you select rare values, Splunk will automatically pipe your search results to the rare command, which shows the least common values of a field2. Therefore, option B is correct, while options A, C and D are incorrect because they do not pipe your search results to the rare command.

QUESTION 64
A report scheduled to run every 15 mins. but takes 17 mins. to complete is in danger of being_____.

A. skipped or deferred
B. automatically accelerated
C. deleted

D. all of the above

Correct Answer: A
Section:
Explanation:
A report that is scheduled to run every 15 minutes but takes 17 minutes to complete is in danger of being skipped or deferred2.This means that Splunk may skip some scheduled runs of the report if they overlap with previous runs that are still in progress or defer them until the previous runs are finished2.This can affect the accuracy and timeliness of the report results and notifications2. Therefore, option A is correct, while options B, C and D are incorrect because they are not consequences of a report taking longer than its schedule interval.

QUESTION 65
Which of the following are valid options to speed up reports? (Select all the apply.)

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

Correct Answer: C
Section:
Explanation:
One of the valid options to speed up reports is to edit acceleration, which means that you can enable summary indexing or data model acceleration for your reports to improve their performance2.Summary indexing allows you to create reports that run over large amounts of data by storing the results of scheduled searches in a summary index and using that index for faster reporting2.Data model acceleration allows you to create reports that use data models by creating and storing summaries of the data model datasets and using them for faster reporting2. Therefore, option C is correct, while options A, B and D are incorrect because they are not options to speed up reports.

QUESTION 66
Which of the following statements are true for this search? (Select all that apply.) SEARCH: sourcetype=access* |fields action productId status

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

Correct Answer: C
Section:

QUESTION 67
Use the dedup command to _____.

A. Rename a field in the index
B. remove duplicate values
C. provide an additional alias for the field that can D.be used in the search criteria

Correct Answer: B
Section:

QUESTION 68
Which of the following searches will show the number of categoryId used by each host?

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

Correct Answer: B
Section:

QUESTION 69
This clause is used to group the output of a stats command by a specific name.

A. Rex
B. As
C. List
D. By

Correct Answer: B
Section:

QUESTION 70
This function of the stats command allows you to return the middle-most value of field X.

A. Median(X)
B. Eval by X
C. Fields(X)
D. Values(X)

Correct Answer: A
Section:

QUESTION 71
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 72
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 73
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 74
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 75
These users can create global knowledge objects. (Select all that apply.)

A. users
B. power users
C. administrators

Correct Answer: B, C
Section:

QUESTION 76
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 77
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 78
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 79
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 80
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 81
Which of these search strings is NOT valid:

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

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

QUESTION 82
Which command is used to create choropleth maps?

A. geostats
B. cluster
C. geom

Correct Answer: C
Section:

QUESTION 83
which of the following are valid options with the chart command

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

Correct Answer: A, B
Section:

QUESTION 84
The gauge command:

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

Correct Answer: B
Section:

QUESTION 85
What will you learn from the results of the following search?
sourcetype=cisco_esa | transaction mid, dcid, icid | timechart avg(duration)

A. The average time elapsed during each transaction for all transactions
B. The average time for each event within each transaction
C. The average time between each transaction

Correct Answer: A
Section:

QUESTION 86
Which of these is NOT a field that is automatically created with the transaction command?

A. maxcount
B. duration
C. eventcount

Correct Answer: A
Section:

QUESTION 87
How many ways are there to access the Field Extractor Utility?

A. 3
B. 4
C. 1
D. 5

Correct Answer: A
Section:

QUESTION 88
When defining a macro, what are the required elements?

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

Correct Answer: C
Section:
Explanation:
When defining a search macro, the required elements are the name and the definition of the macro. The name is a unique identifier for the macro that can be used to invoke it in other searches. The definition is the search string that the macro expands to when referenced.The arguments, validation expression, and validation error message are optional elements that can be used to customize the macro behavior and input validation2
1: Splunk Core Certified Power User Track, page 9.2: Splunk Documentation, Define search macros in Settings.

QUESTION 89
Which of the following expressions could be used to create a calculated field called gigabytes?

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

Correct Answer: B
Section:

QUESTION 90
Consider the the following search run over a time range of last 7 days:
index=web sourcetype=access_conbined | timechart avg(bytes) by product_nane
Which option is used to change the default time span so that results are grouped into 12 hour intervals?

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

Correct Answer: A
Section:
Explanation:
The span option is used to specify the time span for the timechart command. The span value can be a number followed by a time unit, such as h for hour, d for day, w for week, etc. The span value determines how the data is grouped into time buckets. For example, span=12h means that the data is grouped into 12-hour intervals.The timespan option is not a valid option for the timechart command2
1: Splunk Core Certified Power User Track, page 9.2: Splunk Documentation, timechart command.

QUESTION 91
What commands can be used to group events from one or more data sources?

A. eval, coalesce
B. transaction, stats
C. stats, format
D. top, rare

Correct Answer: B
Section:
Explanation:
The transaction and stats commands are two ways to group events from one or more data sources based on common fields or time ranges. The transaction command creates a single event out of a group of related events, while the stats command calculates summary statistics over a group of events. The eval and coalesce commands are used to create or combine fields, not to group events. The format command is used to format the results of

a subsearch, not to group events.The top and rare commands are used to rank the most or least common values of a field, not to group events23
1: Splunk Core Certified Power User Track, page 9.2: Splunk Documentation, transaction command.3: Splunk Documentation, stats command.

QUESTION 92
Tags can reference which of the following knowledge objects?

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

Correct Answer: B
Section:
Explanation:
Tags are a type of knowledge object that enable you to assign descriptive keywords to events. Tags can reference any of the following knowledge objects: extracted fields, field aliases, calculated fields, lookups, and event types. Tags cannot reference other tags or search macros.Tags are applied to events at search time based on the values of the fields that they reference2
1: Splunk Core Certified Power User Track, page 10.2: Splunk Documentation, About tags and aliases.

QUESTION 93
If a calculated field has the same name as an extracted field, what happens to the extracted field?

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

Correct Answer: A
Section:
Explanation:
When you define a calculated field, you can specify the name of the field that the eval expression will create or modify. If the name of the calculated field matches the name of an existing extracted field, the calculated field will override the extracted field and replace its value with the result of the eval expression. This means that the original value of the extracted field will not be available for searching or analysis.To avoid this, you should use a unique name for your calculated field or use a different name for your extracted field2
1: Splunk Core Certified Power User Track, page 9.2: Splunk Documentation, Configure calculated fields with props.conf.

QUESTION 94
Given the following eval statement:
...| eval fieldl - if(isnotnull(fieldl),fieldl,0), field2 = if(isnull<field2>, 'NO-VALUE', fieid2)
Which of the following is the equivalent using f ilinull?

A. There is no equivalent expression using f ilinull
B. ... t filinull values=(0,'NO-VALUE') fields=(fieldl,field2)
C. ... I filinull value=0 fieldl I fillnull fields
D. ... I fillnull fieldl I filinull value='NO-VALUE' field2

Correct Answer: B
Section:
Explanation:
The fillnull command replaces null values in one or more fields with a specified value. The values option allows you to specify a comma-separated list of values to fill the null values in the corresponding fields. The fields option

allows you to specify a comma-separated list of fields to apply the fillnull command to. The eval statement in the question uses the if and isnull functions to check if field1 and field2 have null values and replace them with 0 and ''NO-VALUE'' respectively.The equivalent expression using fillnull is to use the values option to specify 0 and ''NO-VALUE'' and the fields option to specify field1 and field22
1: Splunk Core Certified Power User Track, page 9.2: Splunk Documentation, fillnull command.

QUESTION 95
Why are tags useful in Splunk?

A. Tags look for less specific data.
B. Tags visualize data with graphs and charts.
C. Tags group related data together.
D. Tags add fields to the raw event data.

Correct Answer: C
Section:
Explanation:
Tags are a type of knowledge object that enable you to assign descriptive keywords to events based on the values of their fields. Tags can help you to search more efficiently for groups of event data that share common characteristics, such as functionality, location, priority, etc. For example, you can tag all the IP addresses of your routers as router, and then search for tag=router to find all the events related to your routers. Tags can also help you to normalize data from different sources by using the same tag name for equivalent field values.For example, you can tag the field values error, fail, and critical as severity=high, and then search for severity=high to find all the events with high severity level2
1: Splunk Core Certified Power User Track, page 10.2: Splunk Documentation, About tags and aliases.

QUESTION 96
The Splunk Common Information Model (CIM) is a collection of what type of knowledge object?

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

Correct Answer: D
Section:
Explanation:
The Splunk Common Information Model (CIM) is a collection of data models that apply a common structure and naming convention to data from any source. A data model is a type of knowledge object that defines the structure and relationships of fields in a dataset. A data model can have one or more datasets, which are subsets of the data model that represent different aspects of the data. For example, the Network Traffic data model has datasets such as All Traffic, DNS, HTTP, etc. The CIM contains 28 pre-configured data models that cover various domains such as authentication, network traffic, web, email, etc.The CIM is implemented as an add-on that contains the JSON files for the data models, documentation, and tools that support the consistent, normalized treatment of data for maximum efficiency at search time23
1: Splunk Core Certified Power User Track, page 10.2: Splunk Documentation, Overview of the Splunk Common Information Model1.3: Splunkbase, Splunk Common Information Model (CIM)2.

QUESTION 97
To create a tag, which of the following conditions must be met by the user?

A. Identify at least one field:value pair.
B. Have the Power role at a minimum.
C. Be able to edit the sourcetype the tag applies to.
D. Must have the tag capability associated with their user role.

Correct Answer: D

Section:
Explanation:
To create a tag, the user must have the tag capability associated with their user role. The tag capability allows the user to create, edit, and delete tags. The user does not need to identify a field:value pair, have the Power role, or be able to edit the sourcetype the tag applies to. Reference SeeDefine and manage tags in Settingsand [About capabilities] in the Splunk Documentation.

QUESTION 98
Which of the following data models are included in the Splunk Common Information Model (CIM) add-on? (select all that apply)

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

Correct Answer: B, D
Section:
Explanation:
The Splunk Common Information Model (CIM) Add-on includes a variety of data models designed to normalize data from different sources to allow for cross-source reporting and analysis. Among the data models included, Alerts (Option B) and Email (Option D) are part of the CIM. The Alerts data model is used for data related to alerts and incidents, while the Email data model is used for data pertaining to email messages and transactions. User permissions (Option A) and Databases (Option C) are not data models included in the CIM; rather, they pertain to aspects of data access control and specific types of data sources, respectively, which are outside the scope of the CIM's predefined data models.

QUESTION 99
When would transaction be used instead of stats?

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

Correct Answer: D
Section:
Explanation:
The transaction command is used to group events that are related by some common fields or conditions, such as start/end values, time span, or pauses. The stats command is used to calculate statistics on a group of events by a common field value.
Reference
Splunk Community
Splunk Transaction - Exact Details You Need

QUESTION 100
Which of the following is true about a datamodel that has been accelerated?

A. They can be used with Pivot, the | tstats command, or the | datamodel command.
B. They can still be used in the Pivot tool but only with the accelerate_pivot capability.
C. They can no longer be used in the Pivot tool.
D. They can be used with the |tstats command, but will only return that data which has been accelerated.

Correct Answer: A
Section:

Explanation:
A data model that has been accelerated can be used with Pivot, the | tstats command, or the | datamodel command (Option A). Acceleration pre-computes and stores results for quicker access, enhancing the performance of searches and analyses that utilize the data model, especially for large datasets. This makes accelerated data models highly efficient for use in various analytical tools and commands within Splunk.

QUESTION 101
Where are the descriptions of the data models that come with the Splunk Common Information Model (CIM) Add-on documented?

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

Correct Answer: B
Section:
Explanation:
The descriptions of the data models that come with the Splunk Common Information Model (CIM) Add-on are documented in the CIM Add-on manual (Option B). This manual provides detailed information about the data models, including their structure, the types of data they are designed to normalize, and how they can be used to facilitate cross-sourcing reporting and analysis.

QUESTION 102
Which of the following is true about data model attributes?

A. They cannot be created within the data model.
B. They can only be added into a root search dataset.
C. They cannot be edited if inherited from a parent dataset.
D. They can be added to a dataset from search time field extractions.

Correct Answer: D
Section:
Explanation:
Data model attributes are fields that are added to a dataset from search time field extractions, calculated fields, lookups, or aliases. They can be created within the data model editor or inherited from a parent dataset. They can be edited or removed unless they are required by the data model. They can be added to any type of dataset, not just root search datasets. Reference SeeAbout data models, [Define data model attributes], and [Edit data model datasets] in the Splunk Documentation.

QUESTION 103
Which of the following describes this search?
New Search
'third_party_outages(EMEA,-24h)'

A. This search will find all events for the third_party_outages event type that have 'EMEA' or '-24h' in the raw event data.
B. This search will run the third_party_outages saved search and filter for events containing 'EMEA' and '-24h' in the raw event data.
C. This search will run the third_party_outages macro and pass the arguments EMEA and -24h to the macro definition.
D. This search will find all events in the third_party_outages index with the tags EMEA and -24h.

Correct Answer: C
Section:
Explanation:
This search will run the third_party_outages macro and pass the arguments EMEA and -24h to the macro definition. A search macro is a reusable chunk of SPL that can be inserted into other searches. A search macro can take arguments that are used to resolve the search string at execution time. The syntax for using a search macro ismacro_name (argument1, argument2, ...). Reference SeeUse search macros in searchesandSearch macro

examplesin the Splunk Documentation.

QUESTION 104
How can an existing accelerated data model be edited?

A. An accelerated data model can be edited once its .tsidx file has expired.
B. An accelerated data model can be edited from the Pivot tool.
C. The data model must be de-accelerated before edits can be made to its structure.
D. It cannot be edited. A new data model would need to be created.

Correct Answer: C
Section:
Explanation:
An existing accelerated data model can be edited, but the data model must be de-accelerated before any structural edits can be made (Option C). This is because the acceleration process involves pre-computing and storing data, and changes to the data model's structure could invalidate or conflict with the pre-computed data. Once the data model is de-accelerated and edits are completed, it can be re-accelerated to optimize performance.

QUESTION 105
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