Splunk

Exam Questions SPLK-1002

Splunk Core Certified Power User Exam

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

   All examinations will be up to date.

* 24/7 Quality Support

   We will provide service round the clock.

* 100% Pass Rate

   Our guarantee that you will pass the exam.

* Unique Gurantee

   If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (Exam Topic 1)
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*

Answer: A

Explanation:
The data model command allows you to run searches on data models that have been accelerated1. The synta 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.

NEW QUESTION 2
- (Exam Topic 1)
A space is an implied _____ in a search string.

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

Answer: B

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

NEW QUESTION 3
- (Exam Topic 1)
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 result
C. .
D. When you have over 1000 events in a transaction.
E. When you need to group based on start and end constraints.

Answer: D

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

NEW QUESTION 4
- (Exam Topic 1)
In which of the following scenarios is an event type more effective than a saved search?

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

Answer: C

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

NEW QUESTION 5
- (Exam Topic 1)
Which of the following statements about tags is true?

A. Tags are case insensitive.
B. Tags are created at index time.
C. Tags can make your data more understandable.

D. Tags are searched by using the syntax tag: : <fieldneme>

Answer: C

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

NEW QUESTION 6
- (Exam Topic 1)
Which of the following Statements about macros is true? (select all that apply)

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

Answer: BC

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

NEW QUESTION 7
- (Exam Topic 1)
Which of the following statements describes macros?

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

Answer: C

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Definesearchmacros
A macro is a reusable search string that can contain any part of a search, such as search terms, commands, arguments, etc. A macro can have a flexible time range that can be specified when the macro is executed. A macro can also have arguments that can be passed to the macro when it is executed. A macro can be created by using the Settings menu or by editing the macros.conf file. A macro does not have to contain the full search, but only the part that needs to be reused. A macro does not have to have a fixed time range, but can use a relative or absolute time range modifier. A macro does not have to contain only a portion of the search, but can contain multiple parts of the search.

NEW QUESTION 8
- (Exam Topic 1)
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.

Answer: B

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.

NEW QUESTION 9
- (Exam Topic 1)
Data model are composed of one or more of which of the following datasets? (select all that apply.)

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

Answer: ABC

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

Data models are collections of datasets that represent your data in a structured and hierarchical way. Data models define how your data is organized into objects and fields. Data models can be composed of one or more of the following datasets:

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

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

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

NEW QUESTION 10
- (Exam Topic 1)
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.

Answer: C

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. Sta 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.

NEW QUESTION 10
- (Exam Topic 1)
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

Answer: ABD

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

NEW QUESTION 14
- (Exam Topic 1)
Which of the following are required to create a POST workflow action?

A. Label, URI, search string.
B. XMI attributes, URI, name.
C. Label, URI, post arguments.
D. URI, search string, time range picker.

Answer: C

Explanation:
POST workflow actions are custom actions that send a POST request to a web server when you click on a field value in your search results. POST workflow actions can be configured with various options, such as label name, base URL, URI parameters, post arguments, app context, etc. One of the options that are required to create a POST workflow action is post arguments. Post arguments are key-value pairs that are sent in the body of the POST request to provide additional information to the web server. Post arguments can include field values from your data by using dollar signs around the field names.

NEW QUESTION 19
- (Exam Topic 1)
Selected fields are displayed _____ each event in the search results.

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

Answer: A

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.

NEW QUESTION 20
- (Exam Topic 1)
A field alias has been created based on an original field. A search without any transforming commands is then executed in Smart Mode. Which field name appears in the results?

A. Both will appear in the All Fields list, but only if the alias is specified in the search.
B. Both will appear in the Interesting Fields list, but only if they appear in at least 20 percent of events.
C. The original field only appears in All Fields list and the alias only appears in the Interesting Fields list.
D. The alias only appears in the All Fields list and the original field only appears in the Interesting Fields list.

Answer: B

Explanation:
A field alias is a way to assign an alternative name to an existing field without changing the original field name or value2. You can use field aliases to make your field names more consistent or descriptive across
different sources or sourcetypes2. When you run a search without any transforming commands in Smart Mode Splunk automatically identifies and displays interesting fields in your results2. Interesting fields are fields that appear in at least 20 percent of events or have high variability among values2. If you have created a field alias based on an original field, both the original field name and the alias name will appear in the Interesting Fields list if they meet these criteria2. However, only one of them will appear in each event depending on which one you have specified in your search string2. Therefore, option B is correct, while options A, C and D are incorrect.

NEW QUESTION 21
- (Exam Topic 1)
Which of the following statements describe the Common Information Model (CIM)? (select all that apply)

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

Answer: ABC

Explanation:
Reference: https://docs.splunk.com/Documentation/CIM/4.15.0/User/Overview
The Common Information Model (CIM) is a methodology for normalizing data from different sources and making it easier to analyze and report on it3. The CIM defines a common set of fields and tags for various domains such as Alerts, Email, Database, Network Traffic, Web and more3. One of the statements that describe the CIM is that it is a methodology for normalizing data, which means that it provides a standard way to name and structure data from different sources so that they can be compared and correlated3. Therefore, option A is correct. Another statement that describes the CIM is that it can correlate data from different sources, which means that it enables you to run searches and reports across data from different sources that share common fields and tags3. Therefore, option B is correct. Another statement that describes the CIM is that the Knowledge Manager uses the CIM to create knowledge objects, which means that the person who is responsible for creating and managing knowledge objects such as data models, field aliases, tags and event types can use the CIM as a guide to make their knowledge objects consistent and compatible with other apps and add-ons3. Therefore, option C is correct. Option D is incorrect because it does not describe the CIM but rather one of its components.

NEW QUESTION 26
- (Exam Topic 1)
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.

Answer: A

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

NEW QUESTION 27
- (Exam Topic 1)
Which are valid ways to create an event type? (select all that apply)

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

Answer: CD

Explanation:
Event types are custom categories of events that are based on search criteria. Event types can be used to label events with meaningful names, such as error, success, login, logout, etc. Event types can also be used to create transactions, alerts, reports, dashboards, etc. Event types can be created in two ways:
➤ By going to the Settings menu and clicking Event Types > New. This will open a form where you can enter the name, description, search string, app context, and tags for the event type.

⟩ By selecting an event in search results and clicking Event Actions > Build Event Type. This will open a dialog box where you can enter the name and description for the event type. The search string will be automatically populated based on the selected event.

Event types cannot be created by using the searchtypes command in the search bar, as this command does not exist in Splunk. Event types can also be created by editing the event_type stanza in the transforms.conf file, not the props.conf file.

NEW QUESTION 29
- (Exam Topic 1)
Which of the following statements describe the search below? (select all that apply) Index=main I transaction clientip host maxspan=30s maxpause=5s

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

Answer: ABD

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

⟩ It filters the events by the index main, which is a default index in Splunk that contains all data that is not sent to other indexes.

⟩ It uses the transaction command to group events into transactions based on two fields: clientip and host.
The transaction command creates new events from groups of events that share the same clientip and host values.

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

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

NEW QUESTION 33
- (Exam Topic 1)
Which delimiters can the Field Extractor (FX) detect? (select all that apply)

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

Answer: BCD

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/FXSelectMethodstep
The Field Extractor (FX) is a tool that helps you extract fields from your data using delimiters or regular expressions. Delimiters are characters or strings that separate fields in your data. The FX can detect some common delimiters automatically, such as pipes (|), spaces ( ), commas (,), semicolons (;), etc. The FX cannot detect tabs (\t) as delimiters automatically, but you can specify them manually in the FX interface.

NEW QUESTION 38
- (Exam Topic 1)
What are the two parts of a root event dataset?

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

Answer: C

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

NEW QUESTION 40
- (Exam Topic 1)
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.

Answer: ACD

Explanation:

Reference: https://www.edureka.co/blog/splunk-events-event-types-and-tags/
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.

NEW QUESTION 43
- (Exam Topic 1)
Which of the following describes the Splunk Common Information Model (CIM) add-on?

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

Answer: C

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

NEW QUESTION 47
- (Exam Topic 1)
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.

Answer: A

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.

NEW QUESTION 48
- (Exam Topic 1)
Which of the following statements describe calculated fields? (select all that apply)

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

Answer: ABD

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/definecalcfields
Calculated fields are fields that are created by performing calculations on existing fields using the eval command. Calculated fields can be used in the search bar to filter and transform events based on the calculated values. Calculated fields can also be based on an extracted field, which is a field that is extracted from raw data using various methods, such as regex, delimiters, lookups, etc. Calculated fields are not shortcuts for performing calculations using the eval command, but rather results of performing calculations using the eval command. Calculated fields can be applied to any field in Splunk, not only host and sourcetype.
Therefore, statements A, B, and D are true about calculated fields.

NEW QUESTION 53
- (Exam Topic 1)
What does the Splunk Common Information Model (CIM) add-on include? (select all that apply)

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

Answer: BC

Explanation:
The Splunk Common Information Model (CIM) add-on is a collection of pre-built data models and knowledge objects that help you normalize your data from different sources and make it easier to analyze and report on it3. The CIM add-on includes pre-configured data models that cover various domains such as Alerts, Email, Database, Network Traffic, Web and more3. Therefore, option B is correct. The CIM add-on also includes fields and event category tags that define the

common attributes and labels for the data models3. Therefore, option C is correct. The CIM add-on does not include custom visualizations or automatic data model acceleration. Therefore, options A and D are incorrect.

NEW QUESTION 56
- (Exam Topic 1)
When creating a Search workflow action, which field is required?

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

Answer: A

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

NEW QUESTION 57
- (Exam Topic 2)
The timechart command is an example of which of the following command types?

A. Orchestrating
B. Transforming
C. Statistical
D. Generating

Answer: B

Explanation:
The correct answer is B. Transforming. The explanation is as follows:

> The timechart command is a Splunk command that creates a time series chart with corresponding table of statistics12.

> A timechart is a statistical aggregation applied to a field to produce a chart, 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.

> Transforming commands are commands that change the format of the search results into a data structure that can be easily visualized3. Transforming commands often use stats functions to aggregate and summarize data3.

> Therefore, the timechart command is an example of a transforming command, as it transforms the search results into a chart and a table using stats functions123.

NEW QUESTION 58
- (Exam Topic 2)
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)

Answer: A

NEW QUESTION 60
- (Exam Topic 2)
When using a field value variable with a Workflow Action, which punctuation mark will escape the data

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

Answer: B

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

NEW QUESTION 64

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

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

Answer: D

Explanation:
The correct answer is D. field2 values are replaced with the value of the field1.
A field alias is a way to associate an additional (new) name with an existing field name. A field alias can be used to normalize fields from different sources that have different names but represent the same data. Field aliases can also be used to rename fields for clarity or convenience1.
When you create a field alias in Splunk Web, you can select the Overwrite Field Values option to change the behavior of the field alias. This option affects how the Splunk software handles situations where the original field has no value or does not exist, as well as situations where the alias field already exists as a field in your events, alongside the original field2.
If you select the Overwrite Field Values option, the following rules apply:

> If the original field does not exist or has no value in an event, the alias field is removed from that event.

> If the original field and the alias field both exist in an event, the value of the alias field is replaced with the value of the original field.

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

> If the original field does not exist or has no value in an event, the alias field is unchanged in that event.

> If the original field and the alias field both exist in an event, both fields are retained with their respective values.

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

> About calculated fields

> About field aliases

> Create field aliases in Splunk Web

NEW QUESTION 68
- (Exam Topic 2)
In this search, _____ will appear on the y-axis. SEARCH: sourcetype=access_combined status!=200 | chart count over host

A. status
B. host
C. count

Answer: C

Explanation:
In this search, count will appear on the y-axis2. This search uses the chart command to create a chart of the count of events over host for events that have status not equal to 2002. The chart command creates a table with one column for each value of the field after the over clause and one row for each value of the field after the by clause (if any)2. The values in the table are calculated by applying the function before the over clause to the events in each group2. In this case, the chart command creates a table with one column for each host and one row for the count of events for each host. The y-axis of the chart shows the values of the count function applied to each host. Therefore, option C is correct, while options A and B are incorrect because they appear on the x-axis or as labels of the chart.

NEW QUESTION 73
- (Exam Topic 2)
What type of command is eval?

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

Answer: C

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

NEW QUESTION 75
- (Exam Topic 2)
What are the expected results for a search that contains the command | where A=B?

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

Answer: C

Explanation:
The correct answer is C. Events where values of field A are equal to values of field B.
The where command is used to filter the search results based on an expression that evaluates to true or false. The where command can compare two fields, two

values, or a field and a value. The where command can also use functions, operators, and wildcards to create complex expressions1.

The syntax for the where command is:

| where <expression>

The expression can be a comparison, a calculation, a logical operation, or a combination of these. The expression must evaluate to true or false for each event.

To compare two fields with the where command, you need to use the field names without any quotation marks. For example, if you want to find events where the values for the field A match the values for the field

B, you can use the following syntax:

| where A=B

This will return only the events where the two fields have the same value.

The other options are not correct because they use different syntax or fields that are not related to the where command. These options are:

> A. Events that contain the string value where A=B: This option uses the string value where A=B as a search term, which is not valid syntax for the where command. This option will return events that have the literal text "where A=B" in them.

> B. Events that contain the string value A=B: This option uses the string value A=B as a search term, which is not valid syntax for the where command. This option will return events that have the literal text "A=B" in them.

> D. Events where field A contains the string value B: This option uses quotation marks around the value B, which is not valid syntax for comparing fields with the where command. Quotation marks are used to enclose phrases or exact matches in a search2. This option will return events where the field A contains the string value "B".

References:

> where command usage

> Search command cheatsheet

NEW QUESTION 76
- (Exam Topic 2)
Field aliases are used to _____ data

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

Answer: D

NEW QUESTION 79
- (Exam Topic 2)
Which of the following search control will not re-rerun the search? (Select all that apply.)

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

Answer: BCD

Explanation:

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

NEW QUESTION 83
- (Exam Topic 2)
Given the following eval statement:
...| eval fieldl - if(isnotnull(fieldl),fieldl,0), field2 = if(isnull<field2>, "NO-VALUE", fieid2) Which of the following is the equivalent using f ilinull?

A. There is no equivalent expression using f ilinull
B. ... t filinull values=(0,"NO-VALUE") fields=(fieldl,field2)
C. ... I filinull value=0 fieldl I fillnull fields
D. ... I fillnull fieldl I filinull value="NO-VALUE" field2

Answer: B

Explanation:

The fillnull command replaces null values in one or more fields with a specified value. The values option allows you to specify a comma-separated list of values to fill the null values in the corresponding fields. The fields option allows you to specify a comma-separated list of fields to apply the fillnull command to. The eval statement in the question uses the if and isnull functions to check if field1 and field2 have null values and replace them with 0 and "NO-VALUE" respectively. The equivalent expression using fillnull is to use the values option to specify 0 and "NO-VALUE" and the fields option to specify field1 and field22

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

NEW QUESTION 84
- (Exam Topic 2)
What fields does the transaction command add to the raw events? (select all that apply)

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

Answer: BD

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

➤ The transaction command is a Splunk command that finds transactions based on events that meet various constraints12.

➤ Transactions are made up of the raw text (the _raw field) of each member, the time and date fields of the earliest member, as well as the union of all other fields of each member12.

➤ The transaction command adds some fields to the raw events that are part of the transaction123. These fields are:

➤ duration: The difference, in seconds, between the timestamps for the first and last events in the transaction123.

➤ eventcount: The number of events in the transaction123.

➤ transaction_id: A unique identifier for each transaction3. This field is useful for filtering or joining transactions3.

➤ Therefore, the fields that the transaction command adds to the raw events are duration and transaction_id, which are options B and D in your question.

NEW QUESTION 87
- (Exam Topic 2)
We can use the rename command to _____ (Select all that apply.)

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

Answer: D

NEW QUESTION 91
- (Exam Topic 2)
The transaction command allows you to _____ events across multiple sources

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

Answer: B

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.

NEW QUESTION 93
- (Exam Topic 2)
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.

Answer: D

NEW QUESTION 97
- (Exam Topic 2)
This clause is used to group the output of a stats command by a specific name.

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

Answer: B

NEW QUESTION 102
- (Exam Topic 2)
The macro weekly_sales (2) contains the search string:
index—games I eval Product Sales = $price$ $AmountS01d$ Which of the following will return results?

A. 'weekly_sales(3.99, 10) '
B. 'weekly_sales(3.99, 10)
C. 'weekly_sales (3.99, 10)
D. 'weekly_sales(3)

Answer: C

Explanation:
The correct answer is C. 'weekly_sales (3.99, 10)'. This is because search macros accept arguments without quotation marks or dollar signs, and the number of arguments must match the number of parameters defined in the macro. The other options are incorrect because they either use quotation marks or dollar signs around the arguments, or they provide a different number of arguments than the macro expects. You can learn more about how to use search macros in searches from the Splunk documentation1.

NEW QUESTION 107
- (Exam Topic 2)
Data models are composed of one or more of which of the following datasets? (select all that apply)

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

Answer: ABC

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

NEW QUESTION 112
- (Exam Topic 2)
The Splunk Common Information Model (CIM) is a collection of what type of knowledge object?

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

Answer: D

Explanation:
The Splunk Common Information Model (CIM) is a collection of data models that apply a common structure and naming convention to data from any source. A data model is a type of knowledge object that defines the structure and relationships of fields in a dataset. A data model can have one or more datasets, which are subsets of the data model that represent different aspects of the data. For example, the Network Traffic data model has datasets such as All Traffic, DNS, HTTP, etc. The CIM contains 28 pre-configured data models that cover various domains such as authentication, network traffic, web, email, etc. The CIM is implemented as an add-on that contains the JSON files for the data models, documentation, and tools that support the consistent, normalized treatment of data for maximum efficiency at search time23
1: Splunk Core Certified Power User Track, page 10. 2: Splunk Documentation, Overview of the Splunk Common Information Model 1. 3: Splunkbase, Splunk Common Information Model (CIM) 2.

NEW QUESTION 113
- (Exam Topic 2)
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

Answer: B

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.

NEW QUESTION 116
- (Exam Topic 2)
What is the Splunk Common Information Model (CIM)?

A. The CIM is a prerequisite that any data source must meet to be successfully onboarded into Splunk.
B. The CIM provides a methodology to normalize data from different sources and source types.
C. The CIM defines an ecosystem of apps that can be fully supported by Splunk.
D. The CIM is a data exchange initiative between software vendors.

Answer: B

Explanation:
The Splunk Common Information Model (CIM) provides a methodology to normalize data from different sources and source types. The CIM defines a common set of fields and tags for different types of data, such as web, network, email, etc. This allows you to search and analyze data from different sources in a consistent way.

NEW QUESTION 120
- (Exam Topic 2)
In the Field Extractor Utility, this button will display events that do not contain extracted fields. Select your answer.

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

Answer: B

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

NEW QUESTION 123
- (Exam Topic 2)
Which of the following commands support the same set of functions?

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

Answer: C

NEW QUESTION 126
- (Exam Topic 2)
Which statement is true?

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

Answer: C

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

NEW QUESTION 131
- (Exam Topic 2)
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.

Answer: A

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

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

Answer: D

Explanation:

> The eval command is a Splunk command that allows you to create or modify fields using expressions .

> The if function is an expression that evaluates a condition and returns a value based on whether the condition is true or false. The syntax of the if function is if(X,Y,Z), where X is the condition, Y is th value to return if X is true, and Z is the value to return if X is false.

> The isnotnull function is an expression that returns true if the argument is not null, and false otherwise The syntax of the isnotnull function is isnotnull(X), where

X is the argument to check.

Therefore, the expression if (isnotnull (src), src, host) returns the value of src if it is not null, and th value of host otherwise. This means that it will provide a new value for host from src if it exist keep the original value of host otherwise.

NEW QUESTION 137
- (Exam Topic 2)
Which of the following statements describes calculated fields?

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

Answer: B

NEW QUESTION 139
- (Exam Topic 2)
Which of the following is true about Pivot?

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

Answer: A

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

NEW QUESTION 141
- (Exam Topic 2)
Which type of visualization shows relationships between discrete values in three dimensions?

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

Answer: C

Explanation:
https://docs.splunk.com/Documentation/DashApp/0.9.0/DashApp/chartsBub

NEW QUESTION 142
- (Exam Topic 2)
Which of the following statements describes the use of the Filed Extractor (FX)?

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

Answer: C

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

NEW QUESTION 147
- (Exam Topic 2)
Which of the following statements describes the use of the Field Extractor (FX)?

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

Answer: C

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

NEW QUESTION 150
- (Exam Topic 2)
Which of the following statements are true for this search? (Select all that apply.)
SEARCH: sourcetype=access* |fields action productId status

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

Answer: C

NEW QUESTION 155
- (Exam Topic 2)
Which type of workflow action sends field values to an external resource (e.g. a ticketing system)?

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

Answer: A

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

NEW QUESTION 156
- (Exam Topic 2)
When should transaction be used?

A. Only in a large distributed Splunk environment.
B. When calculating results from one or more fields.
C. When event grouping is based on start/end values.
D. When grouping events results in over 1000 events in each group.

Answer: C

NEW QUESTION 159
- (Exam Topic 2)
Which of the following objects can a calculated field use as a source?

A. An alias of a field.
B. A field added by an automatic lookup.
C. The tag field.
D. The eventtype field.

Answer: B

Explanation:
The correct answer is B. A field added by an automatic lookup.
A calculated field is a field that is added to events at search time by using an eval expression. A calculated field can use the values of two or more fields that are already present in the events to perform calculations. A calculated field can use any field as a source, as long as the field is extracted before the calculated field is defined1.
An automatic lookup is a way to enrich events with additional fields from an external source, such as a CSV file or a database. An automatic lookup can add fields to events based on the values of existing fields, such as host, source, sourcetype, or any other extracted field2. An automatic lookup is performed before the calculated fields are defined, so the fields added by the lookup can be used as sources for the calculated fields3.
Therefore, a calculated field can use a field added by an automatic lookup as a source. References:
> About calculated fields
> About lookups
> Search time processing

NEW QUESTION 161
- (Exam Topic 2)
Which of the following statements about tags is true? (select all that apply.)

A. Tags are case-insensitive.
B. Tags are based on field/vale pairs.
C. Tags categorize events based on a search.
D. Tags are designed to make data more understandable.

Answer: BD

Explanation:
The following statements about tags are true: tags are based on field/value pairs and tags categorize events based on a search. Tags are custom labels that can be applied to fields or field values to provide additional context or meaning for your data. Tags can be used to filter or analyze your data based on common concepts or themes. Tags can be created by using various methods, such as search commands, configuration files, user interfaces, etc. Some of the characteristics of tags are:

❯ Tags are based on field/value pairs: This means that tags are associated with a specific field name and a specific field value. For example, you can create a tag called "alert" for the field name "status" and the field value "critical". This means that only events that have status=critical will have the "alert" tag applied to them.

❯ Tags categorize events based on a search: This means that tags are defined by a search string that matches the events that you want to tag. For example, you can create a tag called "web" for the search string sourcetype=access_combined. This means that only events that match the search string sourcetype=access_combined will have the "web" tag applied to them.

The following statements about tags are false: tags are case-insensitive and tags are designed to make data more understandable. Tags are case-sensitive and tags are designed to make data more searchable. Tags are case-sensitive: This means that tags must match the exact case of the field name and field value that they are associated with. For example, if you create a tag called "alert" for the field name "status" and the field value "critical", it will not apply to events that have status=CRITICAL or Status=critical. Tags are designed to make data more searchable: This means that tags can help you find relevant events or patterns in your data by using common concepts or themes. For example, if you create a tag called "web" for the search string sourcetype=access_combined, you can use tag=web to find all events related to web activity.

NEW QUESTION 163
- (Exam Topic 2)
Which of the following eval command functions is valid?

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

Answer: D

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

NEW QUESTION 166
- (Exam Topic 2)
When using | timechart by host, which field is represented in the x-axis?

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

Answer: D

Explanation:

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

NEW QUESTION 168
- (Exam Topic 2)
Which of the following examples would use a POST workflow action?

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

Answer: B

Explanation:
The correct answer is B. Use the field values in an HTTP error event to create a new ticket in an external system.
A workflow action is a knowledge object that enables a variety of interactions between fields in events and other web resources. Workflow actions can create HTML links, generate HTTP POST requests, or launch secondary searches based on field values1.
There are three types of workflow actions that can be set up using Splunk Web: GET, POST, and Search2.

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

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

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

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

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

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

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

> Splexicon:Workflowaction

> About workflow actions in Splunk Web

NEW QUESTION 173
- (Exam Topic 2)
Which of the following searches would return a report of sales by product-name?

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

Answer: B

Explanation:

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

NEW QUESTION 174
- (Exam Topic 2)
Which of the following statements about calculated fields in Splunk is true?

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

Answer: B

Explanation:
The correct answer is B. Calculated fields can be chained together to create more complex fields.
Calculated fields are fields that are added to events at search time by using eval expressions. They can be used to perform calculations with the values of two or more fields already present in those events. Calculated fields can be defined with Splunk Web or in the props.conf file. They can be used in searches, reports, dashboards, and data models like any other extracted field1.
Calculated fields can also be chained together to create more complex fields. This means that you can use a calculated field as an input for another calculated field. For example, if you have a calculated field named total that sums up the values of two fields named price and tax, you can use the total field to create another calculated field named discount that applies a percentage discount to the total field. To do this, you need to define the discount field with an eval expression that references the total field, such as:
discount = total * 0.9
This will create a new field named discount that is equal to 90% of the total field value for each event2. References:

> About calculated fields

> Chaining calculated fields

NEW QUESTION 179
- (Exam Topic 2)
How is an event type created from the search window? (select all that apply)

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

Answer: AC

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

NEW QUESTION 183
- (Exam Topic 2)
These users can create global knowledge objects. (Select all that apply.)

A. users
B. power users
C. administrators

Answer: BC

NEW QUESTION 187
- (Exam Topic 2)
When using | timchart by host, which filed is representted in the x-axis?

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

Answer: A

NEW QUESTION 189
- (Exam Topic 2)
Which of the following are valid options to speed up reports? (Select all the apply.)

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

Answer: C

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

NEW QUESTION 191
- (Exam Topic 2)
When defining a macro, what are the required elements?

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

Answer: C

Explanation:
When defining a search macro, the required elements are the name and the definition of the macro. The name is a unique identifier for the macro that can be used to invoke it in other searches. The definition is the search string that the macro expands to when referenced. The arguments, validation expression, and validation error message are optional elements that can be used to customize the macro behavior and input validation2
1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, Define search macros in Settings.

NEW QUESTION 194
- (Exam Topic 2)
This function of the stats command allows you to return the sample standard deviation of a field.

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

Answer: A

NEW QUESTION 198
- (Exam Topic 2)
Which search would limit an "alert" tag to the "host" field?

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

Answer: D

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

NEW QUESTION 199
- (Exam Topic 2)
The limit attribute will _____.

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

Answer: A

NEW QUESTION 203
- (Exam Topic 2)
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

Answer: A

NEW QUESTION 205
- (Exam Topic 2)
Which field will be used to populate the field if the productName and product:d fields have values for a given event?
| eval productINFO=coalesco(productName,productid)

A. Both field values will be used and the product INFO field will become a multivalue field for the given event.
B. The value for the productName field because it appears first.
C. Neither field value will be used and the field will be assigned a NULL value for the given event.
D. The value for the field because it appears second.

Answer: B

Explanation:
The correct answer is B. The value for the productName field because it appears first.
The coalesce function is an eval function that takes an arbitrary number of arguments and returns the first value that is not null. A null value means that the field has no value at all, while an empty value means that the field has a value, but it is "" or zero-length1.
The coalesce function can be used to combine fields that have different names but represent the same data, such as IP address or user name. The coalesce function can also be used to rename fields for clarity or convenience2.
The syntax for the coalesce function is: coalesce(<field1>,<field2>,…)
The coalesce function will return the value of the first field that is not null in the argument list. If all fields are null, the coalesce function will return null.
For example, if you have a set of events where the IP address is extracted to either clientip or ipaddress, you can use the coalesce function to define a new field called ip, that takes the value of either clientip or ipaddress, depending on which is not null:
| eval ip=coalesce(clientip,ipaddress)
In your example, you have a set of events where the product name is extracted to either productName or productid, and you use the coalesce function to define a new field called productINFO, that takes the value of either productName or productid, depending on which is not null:
| eval productINFO=coalesce(productName,productid)
If both productName and productid fields have values for a given event, the coalesce function will return the value of the productName field because it appears first in the argument list. The productid field will be ignored by the coalesce function.
Therefore, the value for the productName field will be used to populate the productINFO field if both fields have values for a given event.
References:
≫ Search Command> Coalesce
≫ USAGE OF SPLUNK EVAL FUNCTION : COALESCE

NEW QUESTION 210
- (Exam Topic 2)
By default search results are not returned in _____ order.

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

Answer: AD

NEW QUESTION 211
- (Exam Topic 2)
What is a limitation of searches generated by workflow actions?

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

Answer: D

NEW QUESTION 216
- (Exam Topic 2)
How is a macro referenced in a search?

A. By using the macroname command.
B. By using the macro command.
C. By enclosing the macro name in backtick characters (').
D. By enclosing the macro name in single-quote characters (').

Answer: C

Explanation:
The correct answer is C. By enclosing the macro name in backtick characters (`).
A macro is a way to reuse a piece of SPL code in different searches. A macro can take arguments, which are variables that can be replaced by different values when the macro is called. A macro can also contain another macro within it, which is called a nested macro1.
To reference a macro in a search, you need to enclose the macro name in backtick characters (). For example, if you have a macro named my_macro` that takes one argument, you can reference it in a search by using the following syntax:
| my_macro(argument) | ...
This will replace the macro name and argument with the SPL code contained in the macro definition. For example, if the macro definition is:
[my_macro(argument)] search sourcetype=$argument$ And you reference it in a search with:
index=main | my_macro(web) | stats count by host
This will expand the macro and run the following SPL code: index=main | search sourcetype=web | stats count by host References:
> Use search macros in searches

NEW QUESTION 218
- (Exam Topic 2)
Which knowledge Object does the Splunk Common Information Model (CIM) use to normalize data. in addition to field aliases, event types, and tags?

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

Answer: B

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

NEW QUESTION 221
- (Exam Topic 2)
When extracting fields, we may choose to use our own regular expressions

A. True
B. False

Answer: A

NEW QUESTION 223
- (Exam Topic 2)
This function of the stats command allows you to identify the number of values a field has.

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

Answer: D

NEW QUESTION 225
- (Exam Topic 2)
Which of the following statements about tags is true?

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

Answer: B

Explanation:

> Tags are a knowledge object that allow you to assign an alias to one or more field values . Tags are applied to events at search time and can be used as search terms or filters .
> Tags can help you make your data more understandable by replacing cryptic or complex field values
with meaningful names . For example, you can tag the value 200 in the status field as success, or value 404 as not_found .

NEW QUESTION 229
- (Exam Topic 2)
Which of the following is NOT a stats function:

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

Answer: B

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

NEW QUESTION 231
- (Exam Topic 2)
The timechart command buckets data in time intervals depending on:

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

Answer: B

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

NEW QUESTION 236
- (Exam Topic 2)
Which statement is true?

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

Answer: C

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

NEW QUESTION 238
- (Exam Topic 2)
Which of the following is a feature of the Pivot tool?

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

Answer: C

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

NEW QUESTION 240
- (Exam Topic 2)
Which knowledge object is used to normalize field names to comply with the Splunk Common Information Model (CIM)?

A. Field alias
B. Event types
C. Search workflow action
D. Tags

Answer:

A

Explanation:
The correct answer is A. Field alias123.
In Splunk, a field alias is a knowledge object that you can use to assign an alternate name to a field3. This can be particularly useful when you want to normalize your data to comply with the Splunk Common Information Model (CIM)12.
The CIM provides a methodology for normalizing values to a common field name1. It acts as a search-time schema to define relationships in the event data while leaving the raw machine data intact2. By using field aliases, you can map vendor fields to common fields that are the same for each data source in a given domain4. This allows you to correlate events from different source types by normalizing these different occurrences to a common structure and naming convention1.

NEW QUESTION 241
- (Exam Topic 2)
The macro weekly sales (2) contains the search string: index=games | eval ProductSales = $Price$ * $AmountSold$
Which of the following will return results?

A. 'weekly sales (3)'
B. 'weekly_sales($3.995, $108)'
C. 'weekly_sales (3.99, 10)'
D. 'weekly sales (3.99, 10)'

Answer: C

Explanation:
To use a search macro in a search string, you need to place a back tick character (`) before and after the macro name1. You also need to use the same number of arguments as defined in the macro2. The macro weekly sales (2) has two arguments: Price and AmountSold. Therefore, you need to provide two values for these arguments when you call the macro.
The option A is incorrect because it uses parentheses instead of back ticks around the macro name. The option B is incorrect because it uses underscores instead of spaces in the macro name. The option D is incorrect because it uses spaces instead of commas to separate the argument values.
Reference: 1 Use search macros in searches - Splunk Documentation 2 Define search macros in Settings - Splunk Documentation

NEW QUESTION 243
- (Exam Topic 2)
which of the following commands are used when creating visualizations(select all that apply.)

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

Answer: ACD

Explanation:
The following commands are used when creating visualizations: geom, geostats, and iplocation. Visualizations are graphical representations of data that show trends, patterns, or comparisons. Visualizations can have different types, such as charts, tables, maps, etc. Visualizations can be created by using various commands that transform the data into a suitable format for the visualization type. Some of the commands that are used when creating visualizations are:

➢ geom: This command is used to create choropleth maps that show geographic regions with different colors based on some metric. The geom command takes a KMZ file as an argument that defines the geographic regions and their boundaries. The geom command also takes a field name as an argument that specifies the metric to use for coloring the regions.

➢ geostats: This command is used to create cluster maps that show groups of events with different sizes and colors based on some metric. The geostats command takes a latitude and longitude field as arguments that specify the location of the events. The geostats command also takes a statistical function as an argument that specifies the metric to use for sizing and coloring the clusters.

➢ iplocation: This command is used to create location-based visualizations that show events with different attributes based on their IP addresses. The iplocation command takes an IP address field as an argument and adds some additional fields to the events, such as Country, City, Latitude, Longitude, etc. The iplocation command can be used with other commands such as geom or geostats to create maps based on IP addresses.

NEW QUESTION 248
- (Exam Topic 2)
Which of the following searches will return events containing a tag named Privileged?

A. tag=Priv
B. tag=Priv*
C. tag=priv*
D. tag=privileged

Answer: B

Explanation:
The tag=Priv* search will return events containing a tag named Privileged, as well as any other tag that starts with Priv. The asterisk (*) is a wildcard character that matches zero or more characters. The other searches will not match the exact tag name.

NEW QUESTION 252
- (Exam Topic 2)
_____ datasets can be added to root dataset to narrow down the search

A. parent
B. extracted
C. event

D. child

Answer: D

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

NEW QUESTION 254
- (Exam Topic 2)
A macro has another macro nested within it, and this inner macro requires an argument. How can the user pass this argument into the SPL?

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

Answer: D

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

NEW QUESTION 258
- (Exam Topic 2)
Which of the following is true about the Splunk Common Information Model (CIM)?

A. The data models included in the CIM are configured with data model acceleration turned off.
B. The CIM contains 28 pre-configured datasets.
C. The CIM is an app that needs to run on the indexer.
D. The data models included in the CIM are configured with data model acceleration turned on.

Answer: D

Explanation:
The Splunk Common Information Model (CIM) is an app that contains a set of predefined data models that apply a common structure and naming convention to data from any source. The CIM enables you to use data from different sources in a consistent and coherent way. The CIM contains 28 pre-configured datasets that cover various domains such as authentication, network traffic, web, email, etc. The data models included in the CIM are configured with data model acceleration turned on by default, which means that they are optimized for faster searches and analysis. Data model acceleration creates and maintains summary data for the data models, which reduces the amount of raw data that needs to be scanned when you run a search using a data model.
Splunk Core Certified Power User Track, page 10. : Splunk Documentation, About the Splunk Common Information Model.

NEW QUESTION 262
- (Exam Topic 2)
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)

Answer: B

NEW QUESTION 266
- (Exam Topic 2)
Why would the following search produce multiple transactions instead of one?

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

| Events (641) | Patterns | Statistics (147) | Visualization |

| 20 Per Page ▾ | ✎ Format | Preview ▾ | ‹ Prev | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | Next › |

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

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

Answer: A

Explanation:
The correct answer is A. The maxspan option is not included1.
In Splunk, the transaction command is used to group events that share common characteristics into a single transaction1. By default, the transaction command groups all matching events into a single transaction1.
However, you can use the maxspan option to limit the time span of the transactions1. If the time span between the first and last event in a transaction exceeds the maxspan value, the transaction command will start a new transaction1.
Therefore, if the maxspan option is not included in the search, the transaction command might produce multiple transactions instead of one if the time span between the first and last event in a transaction exceeds the default maxspan value1.
Here is an example of how you can use the maxspan option in a search:
index=main sourcetype=access_combined | transaction someuniqefield maxspan=1h
In this search, the transaction command groups events that share the same someuniqefield value into a single transaction, but only if the time span between the first and last event in the transaction does not exceed 1 hour1. If the time span exceeds 1 hour, the transaction command will start a new transaction1.

NEW QUESTION 270
- (Exam Topic 2)
What is the correct format for naming a macro with multiple arguments?

A. monthly_sales(argument 1, argument 2, argument 3)
B. monthly_sales(3)
C. monthly_sales[3]
D. monthly_sales[argument 1, argument 2, argument 3)

Answer: C

Explanation:
The correct format for naming a macro with multiple arguments is monthly_sales3. The square brackets indicate that the macro has arguments, and the number indicates how many arguments it has. The arguments are separated by commas when calling the macro, such as monthly_sales[region,salesperson,date].

NEW QUESTION 273
- (Exam Topic 2)
Clicking a SEGMENT on a chart, _____.

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

Answer: C

NEW QUESTION 275
- (Exam Topic 2)
Where are the results of eval commands stored?

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

Answer: A

Explanation:
https://docs.splunk.com/Documentation/Splunk/8.0.2/SearchReference/Eval
The eval command calculates an expression and puts the resulting value into a search results field.

> If the field name that you specify does not match a field in the output, a new field is added to the search results.

> If the field name that you specify matches a field name that already exists in the search results, the results of the eval expression overwrite the values in that field.

NEW QUESTION 278
- (Exam Topic 2)
Which of the following options will define the first event in a transaction?

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

Answer: A

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

> The transaction command is used to find transactions based on events that meet various constraints12.

> Transactions are made up of the raw text (the _raw field) of each member, the time and date fields of the earliest member, as well as the union of all other fields of each member1.

> The startswith option is used to define the first event in a transaction by specifying a search term or an expression that matches the event13.

> For example, | transaction clientip JSESSIONID startswith="view" will create transactions based on the clientip and JSESSIONID fields, and the first event in each transaction will contain the term "view" in the _raw field2.

NEW QUESTION 283
......

Relate Links

100% Pass Your SPLK-1002 Exam with Exambible Prep Materials

https://www.exambible.com/SPLK-1002-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/