Splunk

Exam Questions SPLK-1002

Splunk Core Certified Power User Exam

NEW QUESTION 1
- (Exam Topic 1)
Which of the following statements describes field aliases?

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

Answer: B

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

NEW QUESTION 2
- (Exam Topic 1)
Which of the following can be used with the eval command tostring function (select all that apply)

A. ‘’hex’’
B. ‘’commas’’
C. ‘’Decimal’’
D. ‘’duration’’

Answer: ABD

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

NEW QUESTION 3
- (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.

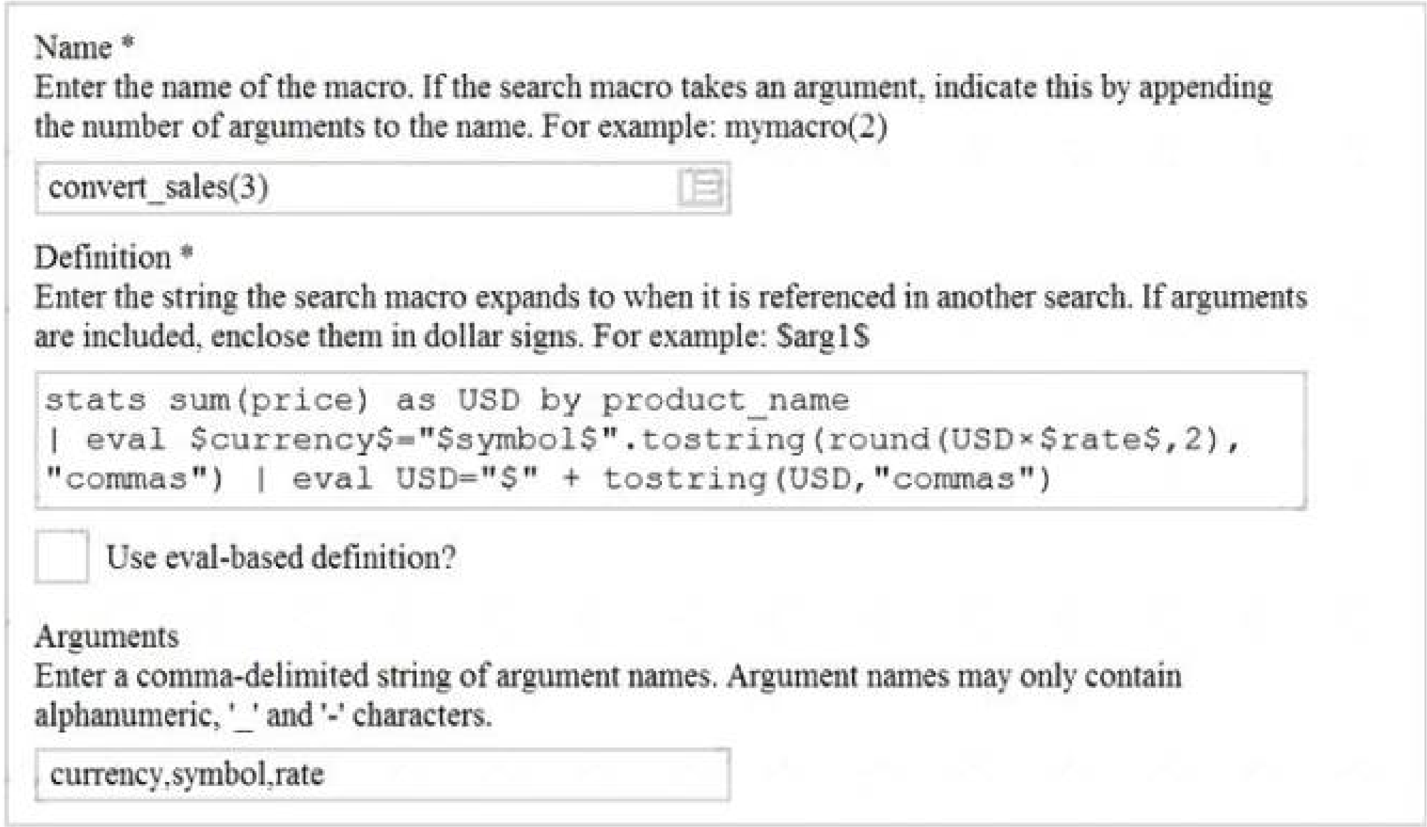
NEW QUESTION 4
- (Exam Topic 1)
When using the Field Extractor (FX), which of the following delimiters will work? (select all that apply)

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 5
- (Exam Topic 1)
Based on the macro definition shown below, what is the correct way to execute the macro in a search string?



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

convert_sales(3)

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

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

□ Use eval-based definition?

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

currency,symbol,rate

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

Answer: B

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

NEW QUESTION 6
- (Exam Topic 1)
In what order arc the following knowledge objects/configurations applied?

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

Answer: B

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

NEW QUESTION 7
- (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 8
- (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 9
- (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 10
- (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 11
- (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 12
- (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 13
- (Exam Topic 2)
Why are tags useful in Splunk?

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

Answer: C

Explanation:
Tags are a type of knowledge object that enable you to assign descriptive keywords to events based on the values of their fields. Tags can help you to search more efficiently for groups of event data that share common characteristics, such as functionality, location, priority, etc. For example, you can tag all the IP addresses of your routers as router, and then search for tag=router to find all the events related to your routers. Tags can also help you to normalize data from different sources by using the same tag name for equivalent field values. For example, you can tag the field values error, fail, and critical as severity=high, and then search for severity=high to find all the events with high severity level2
1: Splunk Core Certified Power User Track, page 10. 2: Splunk Documentation, About tags and aliases.

NEW QUESTION 14
- (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 15
- (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 16
- (Exam Topic 2)
Which is not a comparison operator in Splunk

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

Answer: E

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

NEW QUESTION 17
- (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 18
- (Exam Topic 2)
Which of the following commands will show the maximum bytes?

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

Answer: C

NEW QUESTION 19
- (Exam Topic 2)
Which workflow action type performs a secondary search?

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

Answer: D

Explanation:
The correct answer is D. Search.
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 workflow action type that performs a secondary search is Search. References:

> Splexicon:Workflowaction

> About workflow actions in Splunk Web

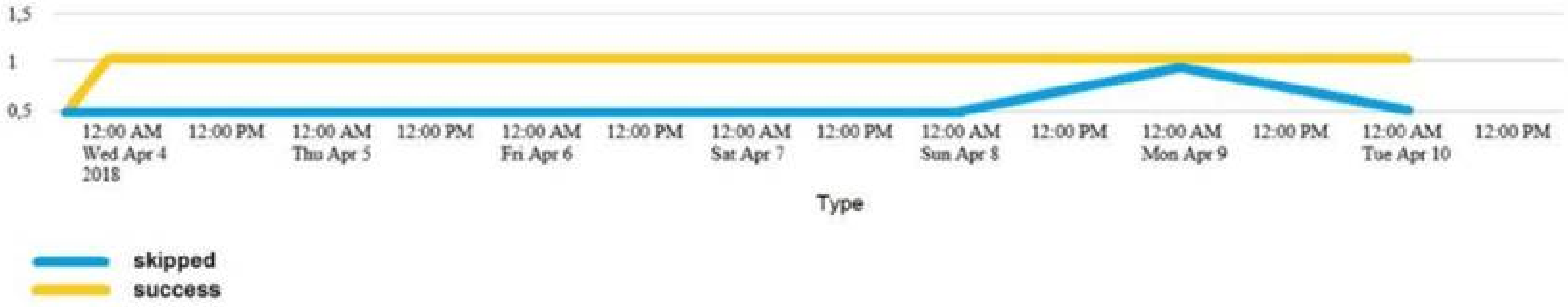
NEW QUESTION 20
- (Exam Topic 2)
Which workflow uses field values to perform a secondary search?

A. POST
B. Action
C. Search
D. Sub-Search

Answer: C

Explanation:
https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/CreateworkflowactionsinSplunkWeb

NEW QUESTION 21
- (Exam Topic 2)
Which of the following searches would create a graph similar to the one below?



A. index_internal seourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan-id | start count states
B. index_internal seourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan-id | chart count states by -time
C. index_internal seourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan-id | timechart count by status

D. None of these searches would generate a similart graph.

Answer: C

Explanation:
The following search would create a graph similar to the one below:
index_internal sourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan=1d | timechart count by status
The search does the following:

- It uses index_internal to specify the internal index that contains Splunk logs and metrics.
- It uses sourcetype=Savesplunker to filter events by the sourcetype that indicates the Splunk Enterprise Security app.
- It uses fields sourcetype, status to keep only the sourcetype and status fields in the events.
- It uses transaction status maxspan=1d to group events into transactions based on the status field with a maximum time span of one day between the first and last events in a transaction.
- It uses timechart count by status to create a time-based chart that shows the count of transactions for each status value over time.

The graph shows the following:

- It is a line graph with two lines, one yellow and one blue.
- The x-axis is labeled with dates from Wed, Apr 4, 2018 to Tue, Apr 10, 2018.
- The y-axis is labeled with numbers from 0 to 15.
- The yellow line represents “shipped” and the blue line represents “success”.
- The yellow line has a steady increase from 0 to 15, while the blue line has a sharp increase from 0 to 5, then a decrease to 0, and then a sharp increase to 10.
- The graph is titled “Type”. Therefore, option C is the correct answer.

NEW QUESTION 22
- (Exam Topic 2)
Which of the following describes the I transaction command?

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

Answer: C

Explanation:

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

NEW QUESTION 23
- (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 24
......