Aug-2024 Get Totally Free Updates on SPLK-1002 Dumps PDF Questions [Q105-Q127

Aug-2024 Get Totally Free Updates on SPLK-1002 Dumps PDF Questions Prepare With Top Rated High-quality SPLK-1002 Dumps For Success in SPLK-1002 Exam

The SPLK-1002 certification exam focuses on various topics related to Splunk, such as searching and reporting, knowledge objects, alerting, and data management. SPLK-1002 exam also covers advanced topics such as creating custom dashboards, data models, and using Splunk's REST API. Splunk Core Certified Power User Exam certification exam is designed to validate the candidate's skills in using Splunk to solve complex problems, making them a valuable asset to any organization. Passing the SPLK-1002 certification exam demonstrates that the candidate has the necessary skills and knowledge to use Splunk effectively and efficiently.

QUESTION 105

Which of the following statements describes an event type?
* A log level measurement: info, warn, error.
* A knowledge object that is applied before fields are extracted.
* A field for categorizing events based on a search string.

* Either a log, a metric, or a trace.
This is because an event type is a knowledge object that assigns a user-defined name to a set of events that match a specific search criteria. For example, you can create an event type named successful_purchase for events that have sourcetype=access_combined, status=200, and action=purchase. Then, you can use eventtype=successful_purchase as a search term to find those events. You can also use event types to create alerts, reports, and dashboards. You can learn more about event types from the Splunk documentation1. The other options are incorrect because they do not describe what an event type is. A log level measurement is a field that indicates the severity of an event, such as info, warn, or error. A knowledge object that is applied before fields are extracted is a source type, which identifies the format and structure of the data. Either a log, a metric, or a trace is a type of data that Splunk can ingest and analyze, but not an event type.

QUESTION 106

Which of the following examples would use a POST workflow action?
* Perform an external IP lookup based on a domain value found in events.
* Use the field values in an HTTP error event to create a new ticket in an external system.
* Launch secondary Splunk searches that use one or more field values from selected events.
* Open a web browser to look up an HTTP status code.
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

QUESTION 107

Which of the following statements would help a user choose between the transaction and stats commands?
* state can only group events using IP addresses.
* The transaction command is faster and more efficient.
* There is a 1000 event limitation with the transaction command.
* Use state when the events need to be viewed as a single event.

Reference:

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

QUESTION 108

Which of the following Statements about macros is true? (select all that apply)
* Arguments are defined at execution time.
* Arguments are defined when the macro is created.
* Argument values are used to resolve the search string at execution time.
* Argument values are used to resolve the search string when the macro is created.

QUESTION 109

The macro weekly_sales (2) contains the search string:

index-games I eval Product Sales = $price$ $AmountS01d$

Which of the following will return results?
* ‘weekly_sales (3.99, 10)
* ‘weekly_sales(3.99, 10) ‘
* ‘weekly_sales(3.99, 10)
* ‘weekly_sales(3)

The correct answer is C. ‘weekly_sales (3.99, 10)’. This is because search macros accept arguments without quotation marks or dollar signs, and the number of arguments must match the number of parameters defined in the macro. The other

options are incorrect because they either use quotation marks or dollar signs around the arguments, or they provide a different number of arguments than the macro expects. You can learn more about how to use search macros in searches from the Splunk documentation1.

QUESTION 110

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

QUESTION 111

How are arguments defined within the macro search string?
* arg$
* ‘arg’
* %arg%
* “arg”
Arguments are defined within the macro search string by using dollar signs on either side of the argument

name, such as arg1 or fragment.

References

Search macro examples

Define search macros in Settings

Use search macros in searches

QUESTION 112

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

QUESTION 113

When you mouse over and click to add a search term this (thesE. Boolean operator(s) is(arE. not implied.

(Select all that apply).
* OR
* ( )
* AND
* NOT

When you mouse over and click to add a search term from the Fields sidebar or from an event in your search results, Splunk automatically adds the term to your search string with an implied ANDoperator2. However, this does not apply to some Boolean operators such as OR, NOT and parentheses (). These operators are not implied when you add a search term and you have to type them manually if you want to use them in your search string2. Therefore, options A, B and D are correct, while option C is incorrect because AND is implied when you add a search term.

QUESTION 114

When using timechart, how many fields can be listed after a byclause?
* 0, because timechart doesn’t support using a by clause.
* 1, because _time is already implied as the x-axis.
* 2, because one field would represent the x-axis and the other would represent the y-axis.
* There is no limit specific to timechart.

QUESTION 115

Which of the following statements describe GET workflow actions?
* GET workflow actions must be configured with POST arguments.
* Configuration of GET workflow actions includes choosing a sourcetype.
* Label names for GET workflow actions must include a field name surrounded by dollar signs.
* GET workflow actions can be configured to open the URT link in the current window or in a new window

Explanation

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

QUESTION 116

Which of the following statements best describes a macro?
* A macro is a method of categorizing events based on a search.
* A macro is a way to associate an additional (new) name with an existing field name.
* A macro is a portion of a search that can be reused in multiple place
* A macro is a knowledge object that enables you to schedule searches for specific events.
The correct answer is C. A macro is a portion of a search that can be reused in multiple places.

A macro is a way to reuse a piece of SPL code in different searches. A macro can be any part of a search, such as an eval statement or a search term, and does not need to be a complete command. A macro can also take arguments, which are variables that can be replaced by different values when the macro is called. A macro can also contain another macro within it, which is called a nested macro1.

To create a macro, you need to define its name, definition, arguments, and description in the Settings > Advanced Search > Search Macros page in Splunk Web or in the macros.conf file. To use a macro in a search, you need to enclose the macro name in backtick characters (`) and provide values for the arguments if any1.

For example, if you have a macro named my_macro that takes one argument named object and has the following definition:

search sourcetype= object

You can use it in a search by writing:

my_macro(web)

This will expand the macro and run the following SPL code:

search sourcetype=web

The benefits of using macros are that they can simplify complex searches, reduce errors, improve readability, and promote consistency1.

The other options are not correct because they describe other types of knowledge objects in Splunk, not macros. These objects are:

* A. An event type is a method of categorizing events based on a search. An event type assigns a label to events that match a specific search criteria. Event types can be used to filter and group events, create alerts, or generate reports2.

* B. A field alias is a way to associate an additional (new) name with an existing field name. A field alias can be used to normalize fields from different sources that have different names but represent the same data. Field aliases can also be used to rename fields for clarity or convenience3.

* D. An alert is a knowledge object that enables you to schedule searches for specific events and trigger actions when certain conditions are met. An alert can be used to monitor your data for anomalies, errors, or other patterns of interest and notify you or others when they occur4.

References:

* About event types

* About field aliases

* About alerts

* Define search macros in Settings

* Use search macros in searches

QUESTION 117

What approach is recommended when using the Splunk Common Information Model (CIM) add-on to normalize data?
* Consult the CIM data model reference tables.
* Run a search using the authentication command.
* Consult the CIM event type reference tables.
* Run a search using the correlation command.

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

QUESTION 118

When used with the timechart command, which value of the limit argument returns all values?
* limit=*
* limit=all
* limit=none
* limit=0

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

QUESTION 119

Which of the following statements would help a user choose between the transactionand stats commands?
* statscan only group events using IP addresses.
* The transactioncommand is faster and more efficient.
* There is a 1000 event limitation with the transactioncommand.
* Use statswhen the events need to be viewed as a single correlated event.

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

QUESTION 120

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?
* An argument can be passed through the outer macro.
* An argument can be passed to the outer macro by nesting parentheses.
* There is no way to pass an argument to the inner macro.
* An argument can be passed to the inner macro by nesting parentheses.

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 namedouter_macro

(1)that contains another search macro namedinner_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

QUESTION 121

The Field Extractor (FX) is used to extract a custom field. A report can be created using this custom field. The created report can then be shared with other people in the organization. If another person in the organization runs the shared report and no results are returned, why might this be? (select all that apply)
* Fast mode is enabled.
* The dashboard is private.
* The extraction is private-
* The person in the organization running the report does not have access to the index.

The Field Extractor (FX) is a tool that helps you extract fields from your events using a graphical interface2. You can create a report using a custom field extracted by the FX and share it with other users in your organization2. However, if another user runs the shared report and no results are returned, there could be two possible reasons. One reason is that the extraction is private, which means that only you can see and use the extracted field2. To make the extraction available to other users, you need to make it global or app-level2.

Therefore, option C is correct. Another reason is that the other user does not have access to the index where the events are stored2. To fix this issue, you need to grant the appropriate permissions to the other user for the index2. Therefore, option D is correct. Options A and B are incorrect because they are not related to the field extraction or the report.

QUESTION 122

Which of the following is the correct way to use the datamodelcommand to search fields in the Webdata model within the Webdataset?
* | datamodel Web Web search | fields Web*
* | search datamodel Web Web | fields Web*
* | datamodel Web Web fields | search Web*
* datamodel=Web | search Web | fields Web*

QUESTION 123

Which of the following can be used with the evalcommand tostringfunction? (Choose all that apply.)
* “hex”
* “commas”
* “decimal”
* “duration”

Explanation

Explanation/Reference: https://splunkonbigdata.com/2018/10/27/usage-of-splunk-eval-function-tostring/

QUESTION 124

These kinds of charts represent a series in a single bar with multiple sections
* Multi-Series
* Split-Series
* Omit nulls
* Stacked

QUESTION 125

Which of the following commands support the same set of functions?

* stats, eval, table
* search, where, eval
* stats, chart, timechart
* transaction, chart, timechart

QUESTION 126

Which of these is NOT a field that is automatically created with the transaction command?
* maxcount
* duration
* eventcount

QUESTION 127

Which of the following searches would create a graph similar to the one below?

* index_internal seourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan-id | start count states
* index_internal seourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan-id | chart count states by -time
* index_internal seourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan-id | timechart count by status
* None of these searches would generate a similart graph.