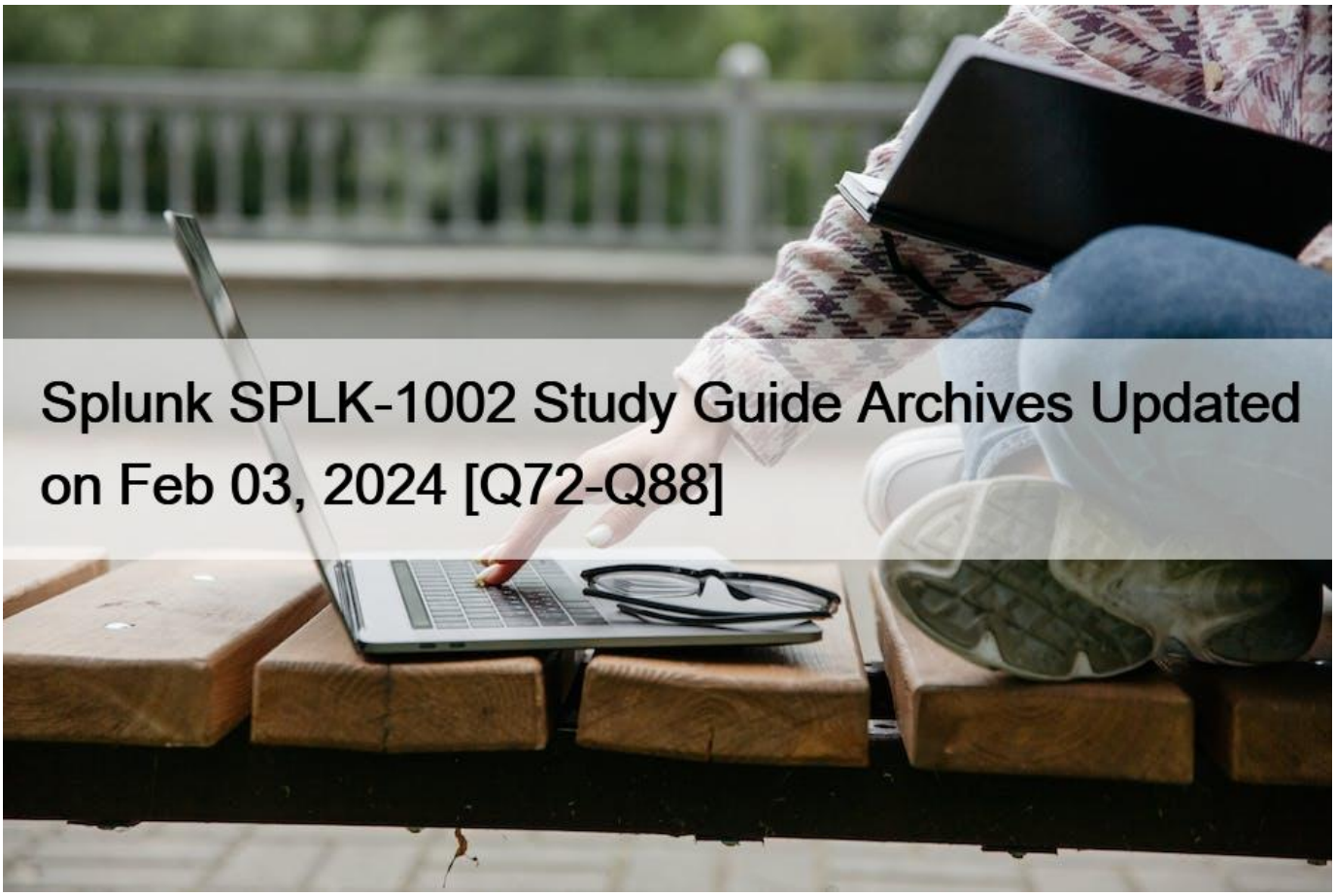
Splunk SPLK-1002 Study Guide Archives Updated on Feb 03, 2024 [Q72-Q88



Splunk SPLK-1002 Study Guide Archives Updated on Feb 03, 2024 Download SPLK-1002 Mock Test Study Material
QUESTION 72

Which of the following statements about tags is true? (select all that apply.)
* Tags are case-insensitive.
* Tags are based on field/vale pairs.
* Tags categorize events based on a search.
* Tags are designed to make data more understandable.

QUESTION 73

Which of the following statements describe the Common Information Model (QM)? (select all that apply)
* CIM is a methodology for normalizing data.
* CIM can correlate data from different sources.
* The Knowledge Manager uses the CIM to create knowledge objects.
* CIM is n app that can coexist with other apps on a single Splunk deployment.

QUESTION 74

Complete the search, …. | _____ failure>successes
* Search
* Where
* If
* Any of the above
The where command can be used to complete the search below.

… | where failure>successes

The where command is a search command that allows you to filter events based on complex or custom criteri a. The where command can use any boolean expression or function to evaluate each event and determine whether to keep it or discard it. The where command can also compare fields or perform calculations on fields using operators such as >, <, =, +, -, etc. The where command can be used after any transforming command that creates a table or a chart.

The search string below does the following:

It uses … to represent any search criteria or commands before the where command.

It uses the where command to filter events based on a comparison between two fields: failure and successes.

It uses the greater than operator (>) to compare the values of failure and successes fields for each event.

It only keeps events where failure is greater than successes.

QUESTION 75

Which of the following statements describe the search below? (select all that apply) Index=main I transaction clientip host maxspan=30s maxpause=5s
* Events in the transaction occurred within 5 seconds.
* It groups events that share the same clientip and host.
* The first and last events are no more than 5 seconds apart.
* The first and last events are no more than 30 seconds apart.
Explanation

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

index=main | transaction clientip host maxspan=30s maxpause=5s

The search does the following:

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

It uses the transaction command to group events into transactions based on two fields: clientip and host.

The transaction command creates new events from groups of events that share the same clientip and host values.

It specifies the start and end constraints for the transactions using the maxspan and maxpause arguments. The maxspan argument sets the maximum time span between the first and last events in a transaction. The maxpause argument sets the maximum time span

between any two consecutive events in a transaction. In this case, the maxspan is 30 seconds and the maxpause is 5 seconds, meaning that any transaction that has a longer time span or pause will be split into multiple transactions.

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

QUESTION 76

Complete the search, …. | _____ failure>successes
* Search
* Where
* If
* Any of the above
Explanation

The where command can be used to complete the search below.

… | where failure>successes

The where command is a search command that allows you to filter events based on complex or custom criteria.

The where command can use any boolean expression or function to evaluate each event and determine whether to keep it or discard it. The where command can also compare fields or perform calculations on fields using operators such as >, <, =, +, -, etc. The where command can be used after any transforming command that creates a table or a chart.

The search string below does the following:

It uses … to represent any search criteria or commands before the where command.

It uses the where command to filter events based on a comparison between two fields: failure and successes.

It uses the greater than operator (>) to compare the values of failure and successes fields for each event.

It only keeps events where failure is greater than successes.

QUESTION 77

A space is an implied _____ in a search string.
* OR
* AND
* ()
* NOT

QUESTION 78

The time range specified for a historical search defines the _____ .——questionable on ans
* Amount of data shown on the timeline as data streams in
* Amount of data fetched from index matching that time range
* Time range for the static results
Explanation

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

QUESTION 79

Which of the following actions can the eval command perform?
* Remove fields from results.
* Create or replace an existing field.
* Group transactions by one or more fields.
* Save SPL commands to be reused in other searches.

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

QUESTION 80

Which of the following statements describes the use of the Filed Extractor (FX)?
* The Field Extractor automatically extracts all field at search time.
* The Field Extractor uses PERL to extract field from the raw events.
* Field extracted using the Extracted persist as knowledge objects.
* Fields extracted using the Field Extractor do not persist and must be defined for each search.

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.

QUESTION 81

Which syntax will find events where the values for the 1 field match the values for the Renewal-MonthYear field?
* | where 10yearAnnerversary=Renewal-MonthYear
* | where ’10yearAnnerversary=Renewal-MonthYear
* | where 10yearAnnerversary=’Renewal-MonthYear’
* | where ’10yearAnnerversary’=’Renewal-MonthYear’

Explanation

The correct answer is A. | where 10yearAnnerversary=Renewal-MonthYear.

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 10yearAnnerversary field match the values for the Renewal-MonthYear field, you can use the following syntax:

| where 10yearAnnerversary=Renewal-MonthYear

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

The other options are not correct because they use quotation marks around the field names, which will cause the where command to interpret them as string values instead of field names. For example, if you use:

| where ’10yearAnnerversary’=’Renewal-MonthYear’

This will return no events because there are no events where the string value ’10yearAnnerversary’ is equal to the string value ‘Renewal-MonthYear’.

References:

where command usage

QUESTION 82

Which of these search strings is NOT valid:
* index=web status=50* | chart count over host, status
* index=web status=50* | chart count over host by status
* index=web status=50* | chart count by host, status

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

QUESTION 83

Which of the following statements describes the use of the Field Extractor (FX)?
* The Field Extractor automatically extracts all fields at search time.
* The Field Extractor uses PERL to extract fields from the raw events.
* Fields extracted using the Field Extractor persist as knowledge objects.
* Fields extracted using the Field Extractor do not persist and must be defined for each search.

Explanation

QUESTION 84

What are the two parts of a root event dataset?
* Fields and variables.
* Fields and attributes.
* Constraints and fields.
* Constraints and lookups.

QUESTION 85

What are the two parts of a root event dataset?
* Fields and variables.
* Fields and attributes.
* Constraints and fields.
* Constraints and lookups.

Reference:https://docs.splunk.com/Documentation/SplunkLight/7.3.5/GettingStarted/Designdatamodelobjects

QUESTION 86

Which of the following statements describe the search string below?

| datamodel Application_State All_Application_State search
* Evenrches would return a report of sales by state.
* Events will be returned from the data model named Application_State.
* Events will be returned from the data model named All_Application_state.
* No events will be returned because the pipe should occur after the datamodel command

Explanation

The search string below returns events from the data model named Application_State.

| datamodel Application_State All_Application_State search

The search string does the following:

It uses the datamodel command to access a data model in Splunk. The datamodel command takes two arguments: the name of the data model and the name of the dataset within the data model.

It specifies the name of the data model as Application_State. This is a predefined data model in Splunk that contains information about web applications.

It specifies the name of the dataset as All_Application_State. This is a root dataset in the data model that contains all events from all child datasets.

It uses the search command to filter and transform the events from the dataset. The search command can use any search criteria or command to modify the results.

Therefore, the search string returns events from the data model named Application_State.

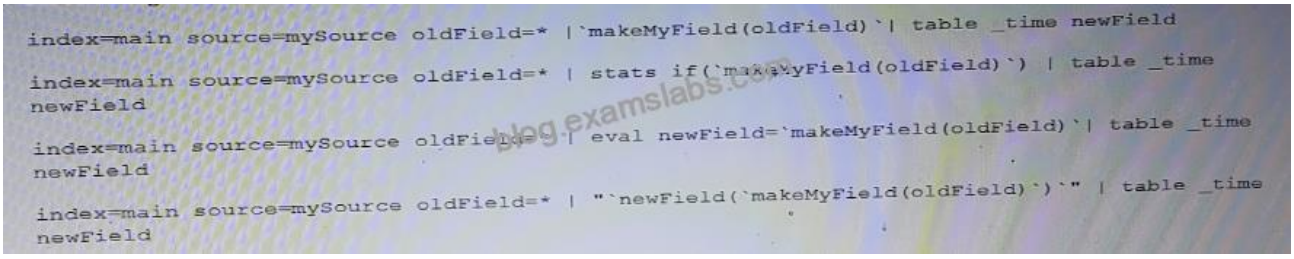
QUESTION 87

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

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

QUESTION 88

Which of the following searches show a valid use of macro? (Select all that apply)



* Option A
* Option B
* Option C
* Option D

SPLK-1002 Questions Prepare with Learning Information:
https://www.examslabs.com/Splunk/Splunk-Core-Certified-Power-User/best-SPLK-1002-exam-dumps.html]