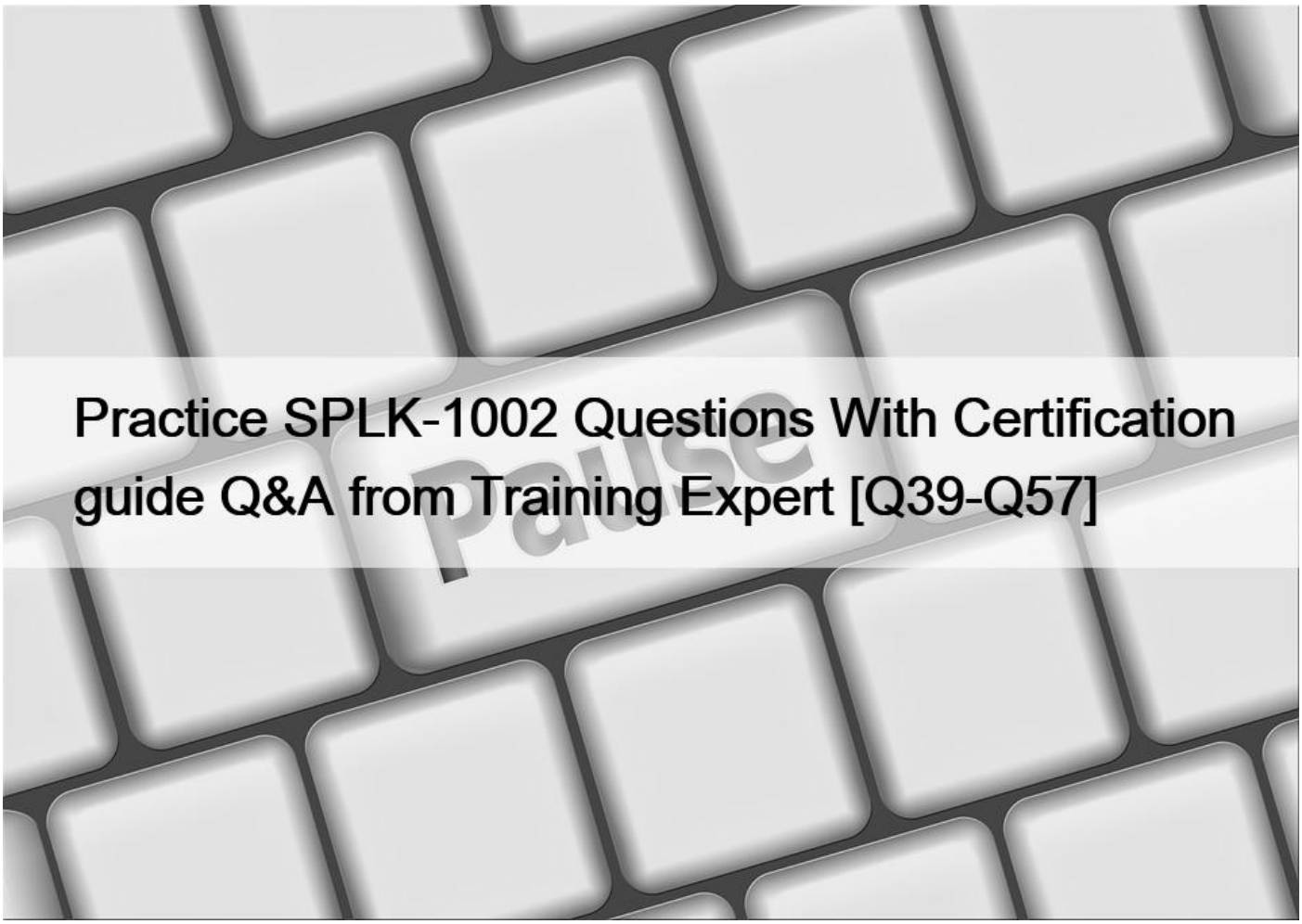
Practice SPLK-1002 Questions With Certification guide Q&A from Training Expert [Q39-Q57



Practice SPLK-1002 Questions With Certification guide Q&A from Training Expert TopExamCollection
Free Splunk SPLK-1002 Test Practice Test Questions Exam Dumps

QUESTION 39

This function of the stats command allows you to identify the number of values a field has.
* max
* distinct_count
* fields
* count

QUESTION 40

The following searches will return the same results. SEARCH 1: ssh error SEARCH 2: ssh AND error
* True

* False

QUESTION 41

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 an app that can coexist with other apps on a single Splunk deployment.

QUESTION 42

What will you learn from the results of the following search? sourcetype=cisco_esa | transaction mid, dcid,

icid | timechart avg(duration)
* The average time elapsed during each transaction for all transactions
* The average time for each event within each transaction
* The average time between each transaction

QUESTION 43

What is required for a macro to accept three arguments?
* The macro’s name ends with (3).
* The macro’s name starts with (3).
* The macro’s argument count setting is 3 or more.
* Nothing, all macros can accept any number of arguments.

QUESTION 44

Which of the following statements describes POST workflow actions?
* Configuration of a POST workflow action includes choosing a sourcetype.
* POST workflow actions can be configured to send email to the URI location.
* By default, POST workflow actions are shown in both the event and field menus.
* POST workflow actions can be configured to send POST arguments to the URI location.

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

QUESTION 45

What does the Splunk Common Information Model (CIM) add-on include? (select all that apply)
* Custom visualizations
* Pre-configured data models
* Fields and event category tags
* Automatic data model acceleration

QUESTION 46

How many ways are there to access the Field Extractor Utility?
* 3
* 4
* 1

* 5

QUESTION 47

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 48

Which statement is true?
* Pivot is used for creating datasets.
* Data model are randomly structured datasets.
* Pivot is used for creating reports and dashboards.
* In most cases, each Splunk user will create their own data model.

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Pivot/IntroductiontoPivot

QUESTION 49

Which command can include both an overand a byclause to divide results into sub-groupings?
* chart
* stats
* xyseries
* transaction

Explanation/Reference: https://www.splunk.com/en_us/blog/tips-and-tricks/search-commands-stats-chart-and- timechart.html

QUESTION 50

_____ datasets can be added to root dataset to narrow down the search
* parent
* extracted
* event
* child

QUESTION 51

What does the fillnull command replace null values with, it the value argument is not specified?
* 0
* N/A
* NaN
* NULL

Reference:

https://answers.splunk.com/answers/653427/fillnull-doesnt-work-without-specfying-a-field.html

QUESTION 52

Which workflow action method can be used when the action type is set to link?
* GET
* PUT
* Search
* UPDATE

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

QUESTION 53

A user wants to convert field values to string and also to sort on those value. Which command should be used first, the eval or the sort?
* It doesn’t matter whether eval or sort is used first.
* Convert the numeric to a string with eval first, then sort.
* Use sort first, then convert the numeric to a string with eval.
* You cannot use the sort command and the eval command on the same field.

QUESTION 54

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 an app that can coexist with other apps on a single Splunk deployment.

Reference:

https://docs.splunk.com/Documentation/CIM/4.15.0/User/Overview

QUESTION 55

When using the transaction command, what does the argument maxspan do?
* Sets the maximum total time between events in a transaction.
* Sets the maximum length of all events within a transaction.
* Sets the maximum total time between the earliest and latest events in a transaction.
* Sets the maximum length that any single event can reach to be included in the transaction.

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

QUESTION 56

In this search, _____ will appear on the y-axis. SEARCH: sourcetype=access_combined status!=200 | chart count over host
* status
* host
* count

QUESTION 57

This search user!=*_____.
* displays only events that contain a value for user
* displays all events
* displays only events that do NOT contain a value for user

Exam Details **SPLK-1002 has 65 multiple-select and multiple-choice questions that should be answered in 57 minutes, with an addition of 3 minutes that are given one to get familiar with the exam agreement. Taking this test will cost $ The applicants will be rated on a variety of knowledge areas, such as the following:** - CIM- Workflow actions- Transformation of commands as well as visualizations- Macros- Knowledge objects

Candidates are advised to take the training courses provided by the vendor when preparing for SPLK-1002 exam. To succeed on the first attempt, they should tackle all the lectures, hands-on sessions, and practice questions to ensure they are adequately ready.

Prepare Top Splunk SPLK-1002 Exam Audio Study Guide Practice Questions Edition:
https://www.topexamcollection.com/SPLK-1002-vce-collection.html]