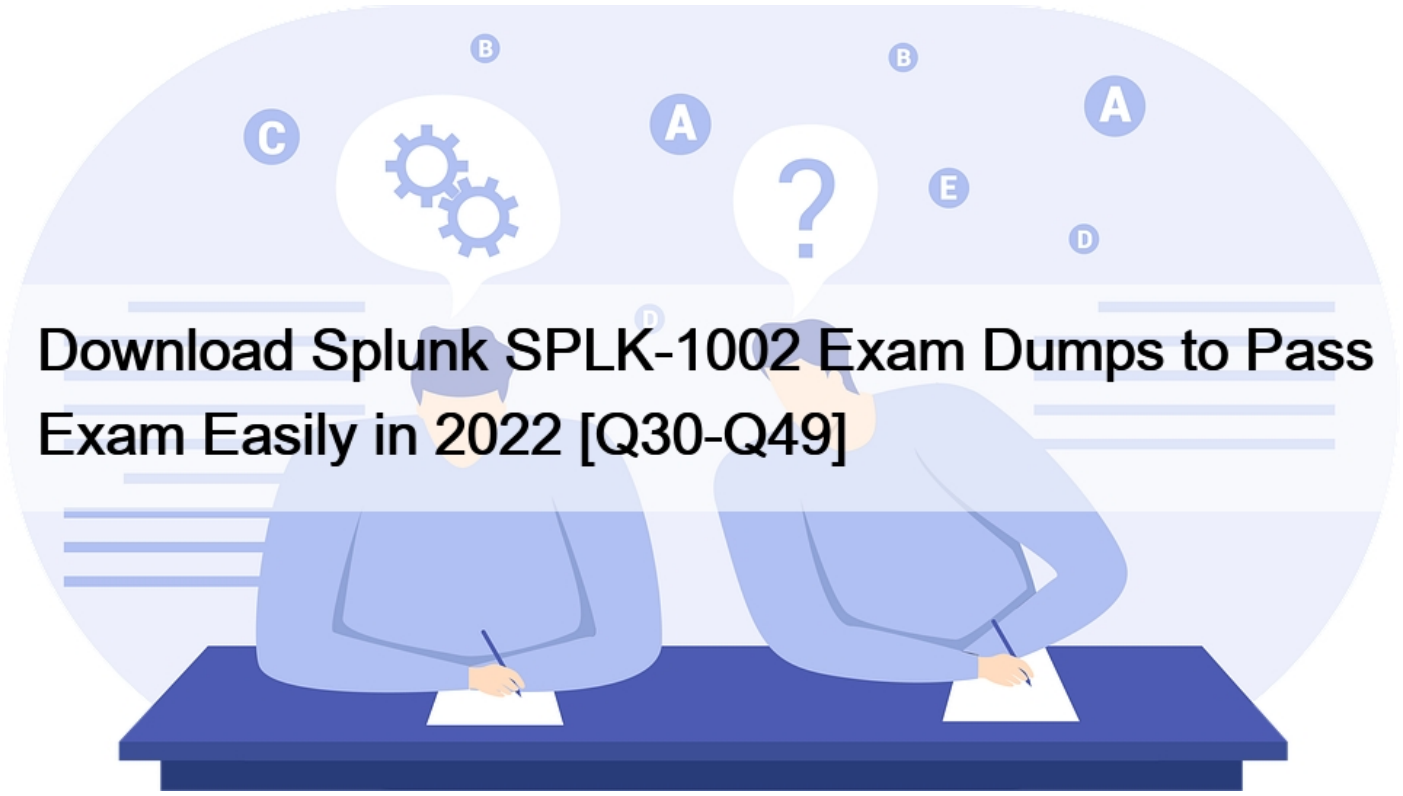
Download Splunk SPLK-1002 Exam Dumps to Pass Exam Easily in 2022 [Q30-Q49



Download Splunk SPLK-1002 Exam Dumps to Pass Exam Easily in 2022
Get 100% Real Free Splunk Core Certified Power User SPLK-1002 Sample Questions

How to book the splk-1002 Exam

These are the following steps for registering the splk-1002 exam:
Step 1: Visit to splk-1002 Exam Registration- Step 2: Signup/Login to Pearson VUE account- Step 3: Search for splk-1002 Certifications Exam- Step 4: Select Date, time and confirm with payment

Certification Path

Splunk Core Certified User is a recommended entry-level exam to Splunk Core Certified Power User. We encourage all candidates to become Splunk Core Certified Users as their first step in our certification program, though it is not required, Candidates can directly appear for Splunk Core Certified Power User splk-1002 Exam.

NO.30 The transaction command allows you to _____ events across multiple sources
* duplicate
* correlate
* persist
* tag

NO.31 Which of the following statements describes the command below (select all that apply) sourcetype-access_combined |

transaction JSESSIONID
* An additional filed named maxspan is created.
* An additional Held named duration is created.
* An additional field named eventcount is created.
* Events with the same JSESSIONID will be grouped together into a single event.

NO.32 Which of the following statements about data models and pivot are true? (select all that apply)
* They are both knowledge objects.
* Data models are created out of datasets called pivots.
* Pivot requires users to input SPL searches on data models.
* Pivot allows the creation of data visualizations that present different aspects of a data model.

NO.33 When should transaction be used?
* Only in a large distributed Splunk environment.
* When calculating results from one or more fields.
* When event grouping is based on start/end values.
* When grouping events results in over 1000 events in each group.

NO.34 When using | timechart by host, which field is represented in the x-axis?
* date
* host
* time
* _time

Reference:

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

NO.35 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.

NO.36 What is the relationship between data models and pivots?
* Data models provide the datasets for pivots.
* Pivots and data models have no relationship.
* Pivots and data models are the same thing.
* Pivots provide the datasets for data models.

NO.37 What does the fillnull command replace null values with, if the value argument is not specified?
* 0
* N/A
* NaN
* NULL

NO.38 To identify all of the contributing events within a transaction that contain at least one REJECTevent, which syntax is correct?
* index=main REJECT | transaction sessionid
* index=main | transaction sessionid | search REJECT
* index=main | transaction sessionid | where transaction=reject

* index=main | transaction sessionid | where transaction=”REJECT*”

NO.39 What does the Splunk Common Information Model (CIM) add-on include? (Choose all that apply.)
* Custom visualizations
* Pre-configured data models
* Fields and event category tags
* Automatic data model acceleration

Explanation/Reference: https://docs.splunk.com/Documentation/CIM/4.18.0/User/Overview

NO.40 Fast, optimized and verbose are all selectable search modes.
* True
* False

NO.41 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 action are shown in both the event and field menus.
* POST workflow actions can be configured to send POST arguments to the URI location.

NO.42 Which of the following searches will return events contains a tag name Privileged?
* Tag= Priv
* Tag= Pri*
* Tag= Priv*
* Tag= Privileged

Reference:https://docs.splunk.com/Documentation/PCI/4.1.0/Install/PrivilegedUserActivity

NO.43 When you mouse over and click to add a search term this (thesE. Boolean operator(s) is(arE. not implied.

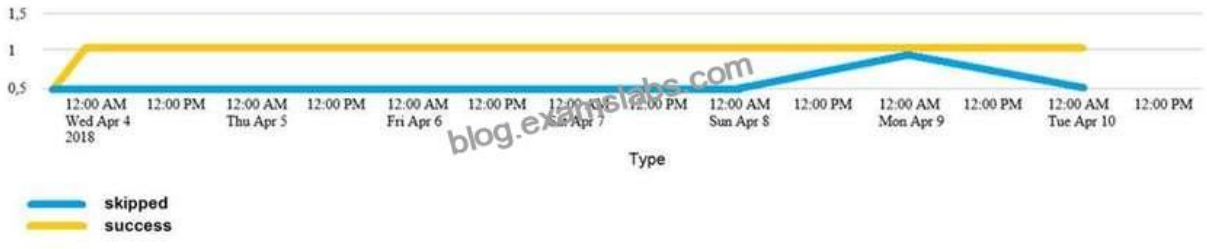
(Select all that apply).
* OR
* ( )
* AND
* NOT

NO.44 When using| timechart by host, which field is represented in the x-axis?
* date
* host
* time
* _time

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

NO.45 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.

NO.46 Which of the following searches would create a graph similar to the one below?



index=_internal sourcetype=SavedSplunker | fields sourcetype, status |
* transaction status maxspan=1d | stats count by status

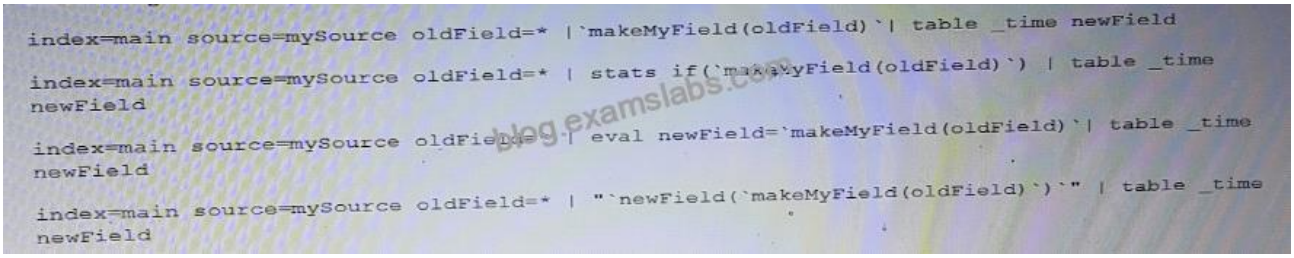
index=_internal sourcetype=SavedSplunker | fields sourcetype, status |
* transaction status maxspan=1d | chart count OVER status by _time

index=_internal sourcetype=SavedSplunker | fields sourcetype, status |
* transaction status maxspan=1d | timechart count by status
* None of these searches would generate a similar graph.

None of these functions related to the graph in exhibit. All of these functions have maxspan=ld which is not a valid argument.

NO.47 What is a limitation of searches generated by workflow actions?
* Searches generated by workflow action cannot use macros.
* Searches generated by workflow actions must be less than 256 characters long.
* Searches generated by workflow action must run in the same app as the workflow action.
* Searches generated by workflow action run with the same permissions as the user running them.

NO.48 Which of the following searches show a valid use of macro? (Select all that apply)



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

NO.49 Data model fields can be added using the Auto-Extracted method. Which of the following statements describe Auto-Extracted fields? (select all that apply)
* Auto-Extracted fields can be hidden in Pivot.
* Auto-Extracted fields can have their data type changed.
* Auto-Extracted fields can be given a friendly name for use in Pivot.
* Auto-Extracted fields can be added if they already exist in the dataset with constraints.

SPLK-1002 Study Guide Realistic Verified Dumps:
https://www.examslabs.com/Splunk/Splunk-Core-Certified-Power-User/best-SPLK-1002-exam-dumps.html]