Exam Splunk SPLK-1002 Demo - Reliable SPLK-1002 Test Book

BONUS!!! Download part of DumpsTorrent SPLK-1002 dumps for free: https://drive.google.com/open?id=1oCR-Lhq8uiZLCvt2eMvEyrUNaHgMT9Ea

After you pay for our SPLK-1002 exam material online, you will get the link to download it in only 5 to 10 minutes. You don't have to wait a long time to start your preparation for the SPLK-1002 exam. And if we have a new version of your SPLK-1002 Study Guide, we will send an E-mail to you. Whenever you have questions about our SPLK-1002 learning quiz, you are welcome to contact us via E-mail. We sincerely offer you 24/7 online service.

Splunk is a powerful platform that helps organizations to analyze and make sense of their machine-generated data. The Splunk Core Certified Power User certification (SPLK-1002) is designed for professionals who want to demonstrate their skills in using the Splunk platform to collect, analyze and visualize data. Splunk Core Certified Power User Exam certification validates the ability to use Splunk's search processing language (SPL) to create complex searches, reports, and dashboards.

>> Exam Splunk SPLK-1002 Demo <<

Reliable SPLK-1002 Test Book, Reliable SPLK-1002 Exam Tips

DumpsTorrent Splunk Core Certified Power User Exam (SPLK-1002) web-based practice exam software also works without installation. It is browser-based; therefore no need to install it, and you can start practicing for the Splunk Core Certified Power User Exam (SPLK-1002) exam by creating the Splunk SPLK-1002 practice test. You don't need to install any separate software or plugin to use it on your system to practice for your actual Splunk Core Certified Power User Exam (SPLK-1002) exam. DumpsTorrent Splunk Core Certified Power User Exam (SPLK-1002) web-based practice software is supported by all well-

known browsers like Chrome, Firefox, Opera, Internet Explorer, etc.

The SPLK-1002 exam is a computer-based exam that consists of 65 multiple-choice and practical lab questions. Candidates have two hours to complete the exam, and they must achieve a minimum score of 70% to pass. SPLK-1002 Exam is available in English, Japanese, and Simplified Chinese, and it can be taken at any Pearson VUE testing center worldwide.

Splunk Core Certified Power User Exam Sample Questions (Q275-Q280):

NEW QUESTION # 275
Information needed to create a GET workflow action includes which of the following? (select all that apply.)

- A. A URI where the user will be directed at search time.
- B. A name for the URI where the user will be directed at search time.
- C. A name of the workflow action
- D. A label that will appear in the Event Action menu at search time.

Answer: A,D

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

NEW QUESTION # 276
A calculated field is a shortcut for performing repetitive, long, or complex transformations using which of the following commands?

- A. eval
- B. stats
- C. lookup
- D. transaction

Answer: A

Explanation:
The correct answer is D. eval.
A calculated field is a field that is added to events at search time by using an eval expression. A calculated field can use the values of two or more fields that are already present in the events to perform calculations. A calculated field can be defined with Splunk Web or in the props.conf file. They can be used in searches, reports, dashboards, and data models like any other extracted field1.
A calculated field is a shortcut for performing repetitive, long, or complex transformations using the eval command. The eval command is used to create or modify fields by using expressions. The eval command can perform mathematical, string, date and time, comparison, logical, and other operations on fields or values2.
For example, if you want to create a new field named total that is the sum of two fields named price and tax, you can use the eval command as follows:
| eval total=price+tax
However, if you want to use this new field in multiple searches, reports, or dashboards, you can create a calculated field instead of writing the eval command every time. To create a calculated field with Splunk Web, you need to go to Settings > Fields > Calculated Fields and enter the name of the new field (total), the name of the sourcetype (sales), and the eval expression (price+tax). This will create a calculated field named total that will be added to all events with the sourcetype sales at search time. You can then use the total field like any other extracted field without writing the eval expression1.
The other options are not correct because they are not related to calculated fields. These options are:
* A. transaction: This command is used to group events that share some common values into a single record, called a transaction. A transaction can span multiple events and multiple sources, and can be
* useful for correlating events that are related but not contiguous3.
* B. lookup: This command is used to enrich events with additional fields from an external source, such as a CSV file or a database. A lookup can add fields to events based on the values of existing fields, such as host, source, sourcetype, or any other extracted field.
* C. stats: This command is used to calculate summary statistics on the fields in the search results, such as count, sum, average, etc. It can be used to group and aggregate data by one or more fields.
References:
* About calculated fields
* eval command overview
* transaction command overview

* [lookup command overview]
* [stats command overview]

NEW QUESTION # 277
Which of the following knowledge objects represents the output of an oval expression?

- A. Field extractions
- B. Calculated fields
- C. Eval fields
- D. Calculated lookups

Answer: B

Explanation:
Reference:https://docs.splunk.com/Splexicon:Calculatedfield

NEW QUESTION # 278
When you mouse over and click to add a search term this (thesE. Boolean operator(s) is(arE. not implied.
(Select all that apply).

- A. ( )
- B. OR
- C. NOT
- D. AND

Answer: A,B,C

Explanation:
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 AND operator2. 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.

NEW QUESTION # 279
What is the correct syntax to find events associated with a tag?

- A. tags=<value>
- B. tag:<field>=<value>
- C. tag=<value>
- D. tags:<field>=<value>

Answer: C

Explanation:
The correct syntax to find events associated with a tag in Splunk istag=<value>1. So, the correct answer isD. tag=<value>.This syntax allows you to annotate specified fields in your search results with tags1.
In Splunk, tags are a type of knowledge object that you can use to add meaningful aliases to field values in your data1. For example, if you have a field calledstatus_codein your data,you might have different status codes like 200, 404, 500, etc. You can create tags for these status codes likesuccessfor 200,not_foundfor 404, andserver_errorfor 500.Then, you can use thetagcommand in your searches to find events associated with these tags1.
Here is an example of how you can use thetagcommand in a search:
index=main sourcetype=access_combined | tag status_code
In this search, thetagcommand annotates thestatus_codefield in the search results with the corresponding tags.If you have tagged the status code 200 withsuccess, the status code 404 withnot_found, and the status code 500 withserver_error, the search results will include these tags1.
You can also use thetagcommand with a specific tag value to find events associated with that tag. For

example, the following search finds all events where the status code is tagged withsuccess:
index=main sourcetype=access_combined | tag status_code | search tag::status_code=success
In this search, thetagcommand annotates thestatus_codefield with the corresponding tags, and thesearchcommand filters the results to include only events where thestatus_codefield is tagged withsuccess1.

NEW QUESTION # 280
.....