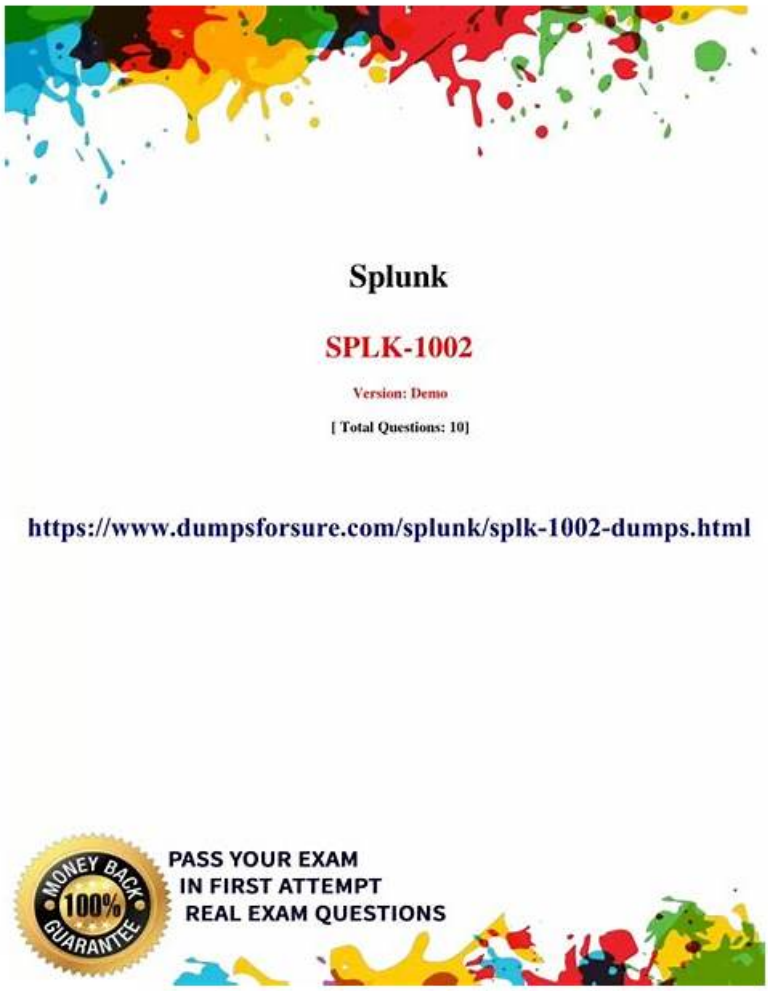
SPLK-1002 Exam Questions And Answers - Test SPLK-1002 Questions Pdf



What's more, part of that 2Pass4sure SPLK-1002 dumps now are free: https://drive.google.com/open?id=1wUelF-EvlYndQfulWsXLEIB7Yny01SYC

There are thousands of customers have passed their SPLK-1002 exam successfully and get the related certification. After that, all of their SPLK-1002 exam torrents were purchase on our website. In addition to the industry trends, the SPLK-1002 test guide is written by lots of past materials' rigorous analyses. The language of our SPLK-1002 Study Materials are easy to be understood, only with strict study, we write the latest and the specialized SPLK-1002 study materials. We want to provide you with the best service and hope you can be satisfied.

The SPLK-1002 Exam covers a range of topics related to the Splunk software, including searching and reporting, user authentication and authorization, knowledge objects, and data management. SPLK-1002 exam also tests the candidate's ability to work with data models, pivot data, and create alerts. Additionally, the exam covers topics related to using Splunk's REST API and Splunk's SDKs.

>> SPLK-1002 Exam Questions And Answers <<

Test SPLK-1002 Questions Pdf & New SPLK-1002 Exam Bootcamp

Candidates can also check the explanations for the answers to have more understanding of the Splunk SPLK-1002 questions that are asked on the SPLK-1002 practice test by 2Pass4sure You can customize the Splunk SPLK-1002 exam questions and time for the SPLK-1002 practice exam on the software. Assessing their Splunk SPLK-1002 Exam Preparation and speed on the practice exam software helps candidates in making required improvements and succeeding at the Splunk SPLK-1002 exam. The software

by 2Pass4sure gives the candidates the results and progress reports to help them monitor their performance for the Splunk SPLK-1002 exam.

The SPLK-1002 certification is an important credential for professionals who use Splunk to analyze and visualize data. Splunk Core Certified Power User Exam certification validates the skills and knowledge needed to effectively use Splunk and can help individuals stand out in a competitive job market. With the right preparation and dedication, candidates can successfully pass the SPLK-1002 Exam and gain the benefits of this valuable certification.

Splunk Core Certified Power User Exam Sample Questions (Q40-Q45):

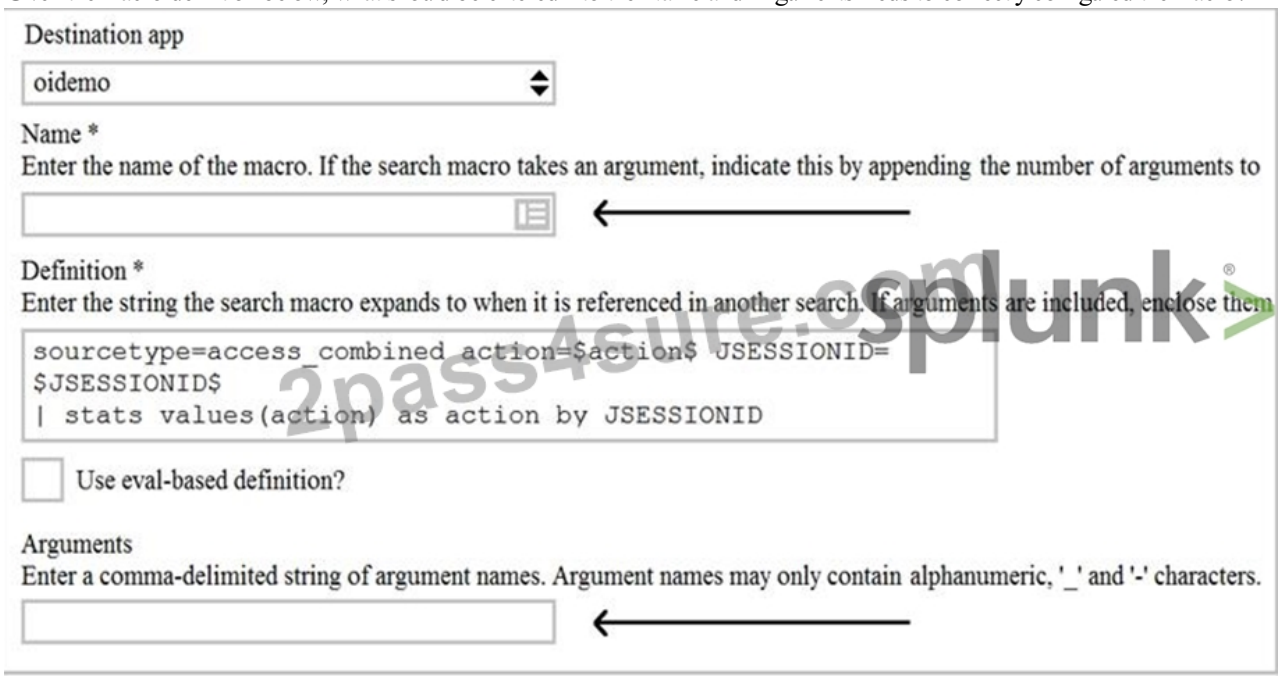
NEW QUESTION # 40
When used with the timechart command, which value of the limit argument returns all values?

- A. limit=*
- B. limit=0
- C. limit=none
- D. limit=all

Answer: B

Explanation:
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.

NEW QUESTION # 41
Given the macro definition below, what should be entered into the Name and Arguments fileds to correctly configured the macro?



- A. The macro name is sessiontracker and the arguments are action, JESSIONID.
- B. The macro name is sessiontracker and the arguments are $action$, $JESSIONID$.
- C. The macro name is sessiontracker(2) and the Arguments are $action$, $JESSIONID$.
- D. The macro name is sessiontracker(2) and the arguments are action, JESSIONID.

Answer: D

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Definesearchmacros The macro definition below

shows a macro that tracks user sessions based on two arguments: action and JSESSIONID.
sessiontracker(2)
The macro definition does the following:
It specifies the name of the macro as sessiontracker. This is the name that will be used to execute the macro in a search string.
It specifies the number of arguments for the macro as 2. This indicates that the macro takes two arguments when it is executed.
It specifies the code for the macro as index=main sourcetype=access_combined_wcookie action=$action$ JSESSIONID=$JSESSIONID$ | stats count by JSESSIONID. This is the search string that will be run when the macro is executed. The search string can contain any part of a search, such as search terms, commands, arguments, etc. The search string can also include variables for the arguments using dollar signs around them.
In this case, action and JSESSIONID are variables for the arguments that will be replaced by their values when the macro is executed.
Therefore, to correctly configure the macro, you should enter sessiontracker as the name and action, JSESSIONID as the arguments. Alternatively, you can use sessiontracker(2) as the name and leave the arguments blank.

NEW QUESTION # 42
Which knowledge Object does the Splunk Common Information Model (CIM) use to normalize data. in addition to field aliases, event types, and tags?

- A. Macros
- B. Field extractions
- C. Workflow actions
- D. Lookups

Answer: D

Explanation:
Explanation
Normalize your data for each of these fields using a combination of field aliases, field extractions, and lookups.
https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsearchtime

NEW QUESTION # 43
A Splunk app is configured to extract domain names in web service logs and specify them as a field named domain.
What workflow action would return an external IP lookup for the field named domain?

- A. PUT
- B. POST
- C. Search
- D. GET

Answer: D

Explanation:
In Splunk, a workflow action that returns an external IP lookup for a field named domain would typically use the GET method. This HTTP method is used to retrieve data from a specified resource, which is appropriate for looking up information based on the domain field.
References:
* Splunk Docs: Define workflow actions
* Splunk Answers: Workflow actions for external lookups

NEW QUESTION # 44
Which of the following statements about event types is true? (select all that apply)

- A. Event types must include a time range,
- B. Event types can be tagged.
- C. Event types can be a useful method for capturing and sharing knowledge.
- D. Event types categorize events based on a search.

Answer: B,C,D

Explanation:
Reference:https://www.edureka.co/blog/splunk-events-event-types-and-tags/
As mentioned before, an event type is a way to categorize events based on a search string that matches the events2. Event types can be tagged, which means that you can apply descriptive labels to event types and use them in your searches2. Therefore, option A is correct. Event types categorize events based on a search string, which means that you can define an event type by specifying a search string that matches the events you want to include in the event type2. Therefore, option C is correct. Event types can be a useful method for capturing and sharing knowledge, which means that you can use event types to organize your data into meaningful categories and share them with other users in your organization2. Therefore, option D is correct. Event types do not have to include a time range, which means that you can create an event type without specifying a time range for the events2. Therefore, option B is incorrect.

NEW QUESTION # 45
.....