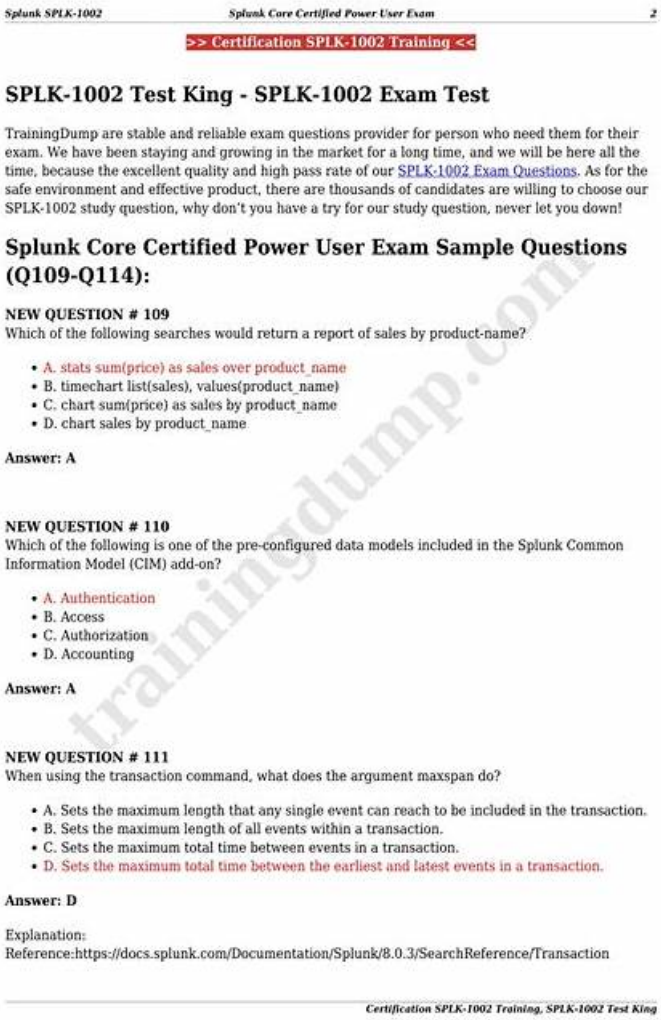
SPLK-1002 Test Question & Valid SPLK-1002 Exam Objectives



Splunk SPLK-1002 Splunk Core Certified Power User Exam 2

>> Certification SPLK-1002 Training <<

SPLK-1002 Test King - SPLK-1002 Exam Test

TrainingDump are stable and reliable exam questions provider for person who need them for their exam. We have been staying and growing in the market for a long time, and we will be here all the time, because the excellent quality and high pass rate of our SPLK-1002 Exam Questions. As for the safe environment and effective product, there are thousands of candidates are willing to choose our SPLK-1002 study question, why don't you have a try for our study question, never let you down!

Splunk Core Certified Power User Exam Sample Questions (Q109-Q114):

NEW QUESTION # 109
Which of the following searches would return a report of sales by product-name?

- A. stats sum(price) as sales over product_name
- B. timechart list(sales), values(product_name)
- C. chart sum(price) as sales by product_name
- D. chart sales by product_name

Answer: A

NEW QUESTION # 110
Which of the following is one of the pre-configured data models included in the Splunk Common Information Model (CIM) add-on?

- A. Authentication
- B. Access
- C. Authorization
- D. Accounting

Answer: A

NEW QUESTION # 111
When using the transaction command, what does the argument maxspan do?

- A. Sets the maximum length that any single event can reach to be included in the transaction.
- B. Sets the maximum length of all events within a transaction.
- C. Sets the maximum total time between events in a transaction.
- D. Sets the maximum total time between the earliest and latest events in a transaction.

Answer: D

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

Certification SPLK-1002 Training, SPLK-1002 Test King

What's more, part of that Real4dumps SPLK-1002 dumps now are free: https://drive.google.com/open?id=1sD9DwMj7DuKxNA_SNANBGMruvdXxqs4Y

Are you still feeling distressed for expensive learning materials? Are you still struggling with complicated and difficult explanations in textbooks? Do you still hesitate in numerous tutorial materials? SPLK-1002 study guide can help you to solve all these questions. SPLK-1002 certification training is compiled by many experts over many years according to the examination outline of the calendar year and industry trends. With SPLK-1002 Study Guide, you only need to spend 20 to 30 hours practicing to take the exam. In addition, SPLK-1002 certification training has a dedicated expert who updates all data content on a daily basis and sends the updated content to the customer at the first time. Therefore, using SPLK-1002 guide torrent, you don't need to worry about missing any exam focus.

It can be said that all the content of the SPLK-1002 prepare questions are from the experts in the field of masterpieces, and these are understandable and easy to remember, so users do not have to spend a lot of time to remember and learn our SPLK-1002 exam questions. It takes only a little practice on a daily basis to get the desired results. Especially in the face of some difficult problems, the user does not need to worry too much, just learn the SPLK-1002 Practice Guide provide questions and answers, you can simply pass the SPLK-1002 exam.

>> SPLK-1002 Test Question <<

Valid SPLK-1002 Exam Objectives, SPLK-1002 Current Exam Content

The SPLK-1002 web-based practice test can accessed online. It means the exam candidates can access it from the browsers like Firefox, Microsoft Edge, Google Chrome, and Safari. The user don't need to install or download any excessive plugins to take the Splunk Core Certified Power User Exam (SPLK-1002) practice test. Mac, Windows, iOS, Android, and Linux support it. The third and last format is the desktop practice test software. The Splunk Core Certified Power User Exam (SPLK-1002) desktop practice test format can be used on Windows computers.

Splunk SPLK-1002 Certification Exam is an industry-recognized certification that validates the expertise of an individual in using Splunk software for data analysis and troubleshooting. Splunk Core Certified Power User Exam certification exam is designed for Splunk power users who want to demonstrate their proficiency in using Splunk's advanced features to optimize and troubleshoot complex deployments.

Splunk Core Certified Power User Exam Sample Questions (Q256-Q261):

NEW QUESTION # 256
What commands can be used to group events from one or more data sources?

- A. eval, coalesce
- B. stats, format
- C. top, rare
- D. transaction, stats

Answer: D

Explanation:
The transaction and stats commands are two ways to group events from one or more data sources based on common fields or time ranges. The transaction command creates a single event out of a group of related events, while the stats command calculates summary statistics over a group of events. The eval and coalesce commands are used to create or combine fields, not to group events. The format command is used to format the results of a subsearch, not to group events. The top and rare commands are used to rank the most or least common values of a field, not to group events23
1: SplunkCore Certified Power User Track, page 9. 2: Splunk Documentation, transaction command. 3: Splunk Documentation, stats command.

NEW QUESTION # 257
Which of the following options will define the first event in a transaction?

- A. firstevent
- B. startingwith
- C. startswith
- D. with

Answer: C

Explanation:
The explanation is as follows:
* The transaction command is used to find transactions based on events that meet various constraints12.
* Transactions are made up of the raw text (the _raw field) of each member, the time and date fields of the earliest member, as well as the union of all other fields of each member1.
* The startswith option is used to define the first event in a transaction by specifying a search term or an expression that matches the event13.
* For example, | transaction clientip JSESSIONID startswith="view" will create transactions based on the clientip and JSESSIONID fields, and the first event in each transaction will contain the term "view" in the _raw field2.

NEW QUESTION # 258
Which statement is true?

- A. Pivot is used for creating datasets.

- B. Pivot is used for creating reports and dashboards.
- C. Data model are randomly structured datasets.
- D. In most cases, each Splunk user will create their own data model.

Answer: B

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

NEW QUESTION # 259
What are search macros?

- A. A method to normalize fields.
- B. Reusable pieces of search processing language.
- C. Lookup definitions in lookup tables.
- D. Categories of search results.

Answer: B

Explanation:
Explanation
The correct answer is B. Reusable pieces of search processing language.
The explanation is as follows:
Search macros are knowledge objects that allow you to insert chunks of SPL into other searches12.
Search macros can be any part of a search, such as an eval statement or a search term, and do not need to be a complete command12.
You can also specify whether the macro field takes any arguments and define validation expressions for them12.
Search macros can help you make your SPL searches shorter and easier to understand3.
To use a search macro in a search string, you need to put a backtick character () before and after the macro name[