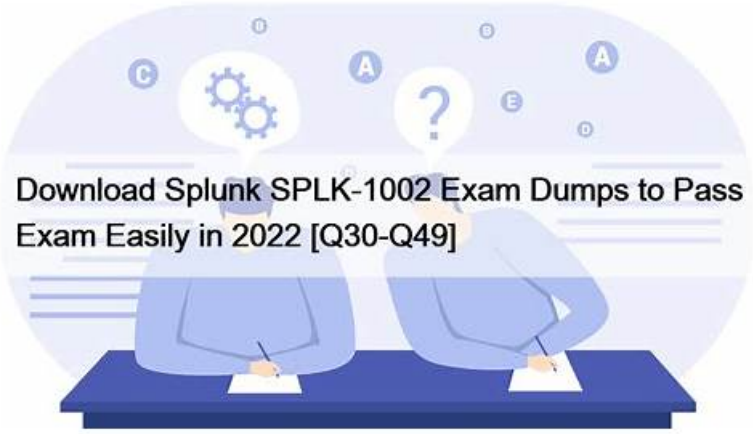
Latest SPLK-1002 Exam Braindumps Materials - SPLK-1002 Test Prep - VCEPrep



P.S. Free & New SPLK-1002 dumps are available on Google Drive shared by VCEPrep: https://drive.google.com/open?id=1GAaVKCbey8eHwrjr8xhddUgNgGqZK1AL

For candidates who buy SPLK-1002 exam bootcamp online, they may have the concern about the money safety. We apply the international recognition third party for the payment, and it will protect the interests of you. Therefore you put your mind at rest if you buy SPLK-1002 exam bootcamp from us. In addition, we have free demo for you to have a try, so that you can have a deeper understanding the complete version of the SPLK-1002 Exam Dumps. If you have any other questions, just contact us, and we will do what we can do to help you.

The benefit in Obtaining the SPLK-1002 Exam Certification

- **splk-1002 Exam** certified individuals would able to have benefits from the stronger community of Splunk, splunk community use to provide support to individuals as and when required.
- Splunk Core Certified Power User Certification provides practical experience to candidates from all the aspects so that they would be a proficient employee in the organization.
- Splunk Core Certified Power User Certifications provide opportunities to get a job.

>> Trustworthy SPLK-1002 Source <<

SPLK-1002 Exam Certification & SPLK-1002 Valid Test Online

With all the information, we can say that your focus should be on real Splunk SPLK-1002 questions of VCEPrep to clear the Splunk Core Certified Power User Exam (SPLK-1002) test. Three formats of the SPLK-1002 exam dumps shall collectively contribute to your success in this regard. In addition, this SPLK-1002 prep material comes with up to 365 days of free Splunk Dumps updates and a free demo.

The Splunk Core Certified Power User Exam certification exam consists of 60 multiple-choice questions, and candidates have 90 minutes to complete the test. SPLK-1002 exam is proctored and can be taken in-person or online. Candidates who pass the exam receive the Splunk Core Certified Power User certification, which is valid for two years.

The SPLK-1002 exam is a 57-question test that must be completed within 90 minutes. SPLK-1002 Exam covers a wide range of topics, including search fundamentals, data analysis, visualization, and troubleshooting. The test is designed to evaluate the candidate's ability to use Splunk to solve real-world problems, and it is ideal for professionals who work with Splunk on a regular basis.

Splunk Core Certified Power User Exam Sample Questions (Q300-Q305):

NEW QUESTION # 300

When does the CIM add-on apply preconfigured data models to the data?

- A. Index time
- B. At midnight
- C. On a cron schedule
- D. Search time

Answer: D

Explanation:
The Common Information Model (CIM) add-on in Splunk applies preconfigured data models to data at search time. This means that when a search is executed, the CIM add-on uses its predefined data models to normalize and map the relevant data to a common format. This approach ensures that data is interpreted and analyzed consistently across various datasets without modifying the data at index time.
References:
* Splunk Docs: About the Common Information Model
* Splunk Answers: CIM Add-on Data Models

NEW QUESTION # 301
Which of the following statements describe GET workflow actions?

- A. GET workflow actions must be configured with POST arguments.
- B. GET workflow actions can be configured to open the URI link in the current window or in a new window.
- C. Label names for GET workflow actions must include a field name surrounded by dollar signs.
- D. Configuration of GET workflow actions includes choosing a sourcetype.

Answer: B

Explanation:
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/8.1.1/Knowledge/SetupaGETworkflowaction

NEW QUESTION # 302
When creating a Search workflow action, which field is required?

- A. An eval statement
- B. Data model name
- C. Search string
- D. Permission setting

Answer: C

NEW QUESTION # 303
Which of the following is NOT a stats function:

- A. sum
- B. addtotals
- C. avg
- D. count

Answer: B

Explanation:
The stats command is used to calculate summary statistics for your search results such as count, sum, avg, min, max and more2. The stats command supports various functions that you can use to perform calculations on your fields2. However, addtotals is not a stats function but a separate command that adds a row or column with the total of the values in each group2. Therefore, option B is correct, while options A, C and D are incorrect because they are valid stats functions.

NEW QUESTION # 304
What is the correct syntax to search for a tag associated with a value on a specific fields?

- A. Tag-<field?
- B. Tag::<filed>=<tagname>
- C. Tag<filed(tagname.)
- D. Tag=<filed>::<tagname>

Answer: B

Explanation:
Reference:https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/TagandaliasfieldvaluesinSplunkWe
A tag is a descriptive label that you can apply to one or more fields or field values in your events2. You can use tags to simplify your searches by replacing long or complex field names or values with short and simple tags2. To search for a tag associated with a value on a specific field, you can use the following syntax: tag::<field>=<tagname>2. For example, tag::status=error will search for events where the status field has a tag named error. Therefore, option D is correct, while options A, B and C are incorrect because they do not follow the correct syntax for searching tags.

NEW QUESTION # 305
.....