New SPLK-1002 Study Materials & Valid Test SPLK-1002 Test

BTW, DOWNLOAD part of Easy4Engine SPLK-1002 dumps from Cloud Storage: https://drive.google.com/open?id=1tQOwiwkU5HVqrkpJSaXAbkm9Lt_5HCOg

Maybe this is the first time you choose our SPLK-1002 practice materials, so it is understandable you may wander more useful information of our SPLK-1002 exam dumps. Those free demos give you simple demonstration of our SPLK-1002 study guide. It is unquestionable necessary for you to have an initial look of them before buying any. They are some brief introductions and basic information but also impressive. Just have a try and you will be interested in them!

The SPLK-1002 Certification Exam is a practical assessment that evaluates your ability to use Splunk to solve real-world problems. SPLK-1002 exam consists of 60 multiple-choice and multiple-select questions that you have to complete within 90 minutes. To pass the exam, you need to score 70% or higher. Splunk Core Certified Power User Exam certification is valid for three years and demonstrates your proficiency in using Splunk to extract insights from data, create dashboards, and automate data analysis workflows.

>> New SPLK-1002 Study Materials <<

SPLK-1002 - Splunk Core Certified Power User Exam –Trustable New Study Materials

The SPLK-1002 web-based practice questions carry the above-mentioned notable features of the desktop-based software. This version of Easy4Engine's SPLK-1002 practice questions works on Mac, Linux, Android, iOS, and Windows. Our customer does not need troubling plugins or software installations to attempt the web-based SPLK-1002 Practice Questions. Another benefit is that our SPLK-1002 online mock test can be taken via all browsers, including Chrome, MS Edge, Internet Explorer, Safari, Opera, and Firefox.

The SPLK-1002 Certification Exam is a comprehensive test designed to evaluate a candidate's proficiency in using Splunk Core. SPLK-1002 exam focuses on the skills and knowledge required to operate and troubleshoot a Splunk environment. Splunk Core Certified Power User Exam certification is aimed at IT professionals, data analysts, and system administrators who work with Splunk and want to demonstrate their expertise in the platform.

Splunk Core Certified Power User Exam Sample Questions (Q279-Q284):

NEW QUESTION # 279
Which of the following data model are included In the Splunk Common Information Model (CIM) add-on? (select all that apply)

- A. Database
- B. Alerts

- C. User permissions
- D. Email

Answer: A,B,D

NEW QUESTION # 280
Given the following eval statement:
... | eval field1 = if(isnotnull(field1),field1,0), field2 = if(isnull(field2), "NO-VALUE", field2) Which of the following is the equivalent using fillnull?

- A. ... | fillnull value=0 field1 | fillnull field2
- B. ... | fillnull values=(0,"NO-VALUE") fields=(field1,field2)
- C. There is no equivalent expression using fillnull
- D. ... | fillnull field1 | fillnull value="NO-VALUE" field2

Answer: A

Explanation:
The fillnull command can be used to replace null values in specific fields. The correct equivalent expression for the given eval statement would involve using fillnull twice, once for field1 to replace null values with 0, and once for field2 to replace null values with "NO-VALUE".
Reference:
Splunk Docs - fillnull command

NEW QUESTION # 281
Which knowledge Object does the Splunk Common Information Model (CIM) use to normalize data. in addition to field aliases, event types, and tags?

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

Answer: A

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 # 282
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)

- A. The dashboard is private.
- B. The extraction is private-
- C. Fast mode is enabled.
- D. The person in the organization running the report does not have access to the index.

Answer: B,D

NEW QUESTION # 283
Splunk alerts can be based on search that run_____. (Select all that apply.)

- A. in real-time

- B. on a regular schedule
- C. and have no matching events

Answer: A,B

Explanation:
Explanation
Splunk alerts can be based on searches that run in real-time or on a regular schedule3. An alert is a way to monitor your data and get notified when certain conditions are met3. You can create an alert by specifying a search and a triggering condition3. You can also specify how often you want to run the search and how you want to receive the alert notifications3. You can run the alert search in real-time, which means that it continuously monitors your data as it streams into Splunk3. Alternatively, you can run the alert search on a regular schedule, which means that it runs at fixed intervals such as every hour or every day3. Therefore, options A and B are correct, while option C is incorrect because it is not a way to run an alert search.

NEW QUESTION # 284

......

Valid Test SPLK-1002 Test: https://www.easy4engine.com/SPLK-1002-test-engine.html