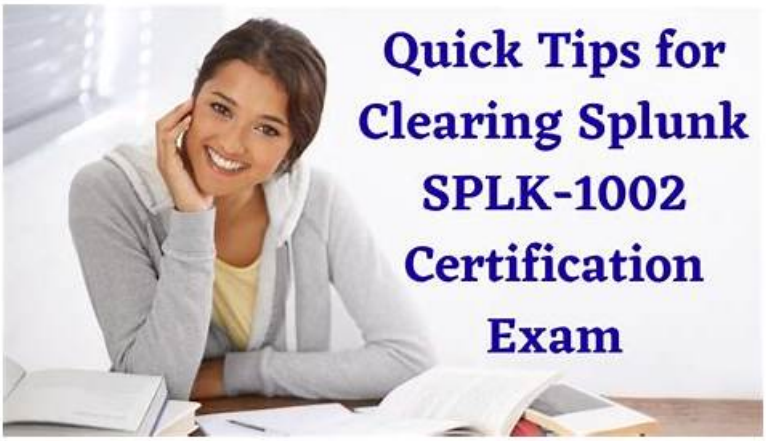
No Internet? No Problem! Prepare For Splunk SPLK-1002 Exam Offline



P.S. Free & New SPLK-1002 dumps are available on Google Drive shared by Actualtests4sure: https://drive.google.com/open?id=1W3O0YXhVe7N4ywD4MDirXG1IvWK3Dcdo

After successful competition of the Splunk SPLK-1002 certification, the certified candidates can put their career on the right track and achieve their professional career objectives in a short time period. For the recognition of skills and knowledge, more career opportunities, professional development, and higher salary potential, the Splunk Core Certified Power User Exam (SPLK-1002) certification exam is the proven way to achieve these tasks quickly.

To earn the Splunk Core Certified Power User certification, individuals must pass the SPLK-1002 exam. SPLK-1002 exam consists of 65 multiple-choice questions and has a time limit of 90 minutes. SPLK-1002 Exam covers various topics, including searching and reporting, creating and managing knowledge objects, and using field aliases and calculated fields.

>> New SPLK-1002 Study Materials <<

Marvelous New SPLK-1002 Study Materials & Leader in Qualification Exams & Hot Pdf SPLK-1002 Exam Dump

If you are a workman and you want to pass SPLK-1002 exam quickly, Actualtests4sure will be your best choice. SPLK-1002 dumps and answers from our Actualtests4sure site are all created by the IT talents with more than 10-year experience in IT certification. It can not only save your time, but also help you pass the SPLK-1002 Exam easily.

Splunk Core Certified Power User Exam Sample Questions (Q121-Q126):

NEW QUESTION # 121
Which of the following data models are included in the Splunk Common Information Model (CIM) add-on?
(select all that apply)

- A. Alerts
- B. User permissions
- C. Email
- D. Databases

Answer: A,C,D

Explanation:
The Splunk Common Information Model (CIM) add-on contains a collection of preconfigured data models that you can apply to your data at search time. Each data model in the CIM consists of a set of field names and tags that define the least common denominator of a domain of interest. The CIM currently has data models defined for 22 categories, including Alerts, Databases, and Email. User permissions is not one of the categories in the CIM.ReferencesSee Overview of the Splunk Common Information Model and Splunk

NEW QUESTION # 122
Which of the following can be used with the eval command tostring function (select all that apply)

- A. "hex"
- B. "commas"
- C. "duration"
- D. "Decimal"

Answer: A,B,C

Explanation:
Reference:
https://splunkonbigdata.com/2018/10/27/usage-of-splunk-eval-function-tostring/

NEW QUESTION # 123
When would a user select delimited field extractions using the Field Extractor (FX)?

- A. When the file has a header that might provide information about its structure or format.
- B. When a log file has values that are separated by the same character, for example, commas.
- C. When a log file contains empty lines or comments.
- D. With structured files such as JSON or XML.

Answer: B

Explanation:
The correct answer is A. When a log file has values that are separated by the same character, for example, commas.
The Field Extractor (FX) is a utility in Splunk Web that allows you to create new fields from your events by using either regular expressions or delimiters. The FX provides a graphical interface that guides you through the steps of defining and testing your field extractions1.
The FX supports two field extraction methods: regular expression and delimited. The regular expression method works best with unstructured event data, such as logs or messages, that do not have a consistent format or structure. You select a sample event and highlight one or more fields to extract from that event, and the FX generates a regular expression that matches similar events in your data set and extracts the fields from them1.
The delimited method is designed for structured event data: data from files with headers, where all of the fields in the events are separated by a common delimiter, such as a comma, a tab, or a space. You select a sample event, identify the delimiter, and then rename the fields that the FX finds1.
Therefore, you would select the delimited field extraction method when you have a log file that has values that are separated by the same character, for example, commas. This method will allow you to easily extract the fields based on the delimiter without writing complex regular expressions.
The other options are not correct because they are not suitable for the delimited field extraction method. These options are:
B) When a log file contains empty lines or comments: This option does not indicate that the log file has a structured format or a common delimiter. The delimited method might not work well with this type of data, as it might miss some fields or include some unwanted values.
C) With structured files such as JSON or XML: This option does not require the delimited method, as Splunk can automatically extract fields from JSON or XML files by using indexed extractions or search-time extractions2. The delimited method might not work well with this type of data, as it might not recognize the nested structure or the special characters.
D) When the file has a header that might provide information about its structure or format: This option does not indicate that the file has a common delimiter between the fields. The delimited method might not work well with this type of data, as it might not be able to identify the fields based on the header information.
Reference:
Build field extractions with the field extractor
Configure indexed field extraction

NEW QUESTION # 124
Which of the following can a field alias be applied to?

- A. Indexes
- B. Event types
- C. Sourcetypes
- D. Tags

Answer: B

Explanation:
Field aliases can be applied at the level of event types to rename or alias fields without modifying the raw data. They do not apply to tags, indexes, or sourcetypes directly.
Reference:
Splunk Power User Study Guide, Knowledge Objects
Splunk Docs: Field Aliases
"Field aliases can be assigned to event types to map one field name to another."

NEW QUESTION # 125
To which of the following can a field alias be applied?

- A. Data found in a lookup table.
- B. Only one single field in a dataset.
- C. Either a calculated field or an extracted field.
- D. A given host, source, or sourcetype.

Answer: C

Explanation:
In Splunk, a field alias is used to create an alternative name for an existing field, making it easier to refer to data in a consistent manner across different searches and reports. Field aliases can be applied to both calculated fields and extracted fields. Calculated fields are those that are created using eval expressions, while extracted fields are typically those parsed from the raw data at index time or search time. This flexibility allows users to streamline their searches by using more intuitive field names without altering the underlying data. Field aliases cannot be applied to data in a lookup table, specific individual fields within a dataset, or directly to a host, source, or sourcetype.

NEW QUESTION # 126
.....

- SPLK-1002 Valid Study Questions □ SPLK-1002 Free Braindumps □ Relevant SPLK-1002 Exam Dumps □ Search for □ SPLK-1002 □ on 「 www.prepawayexam.com 」 immediately to obtain a free download □Online SPLK-1002 Test
- Updated Splunk New SPLK-1002 Study Materials - SPLK-1002 Free Download □ ➽ www.pdfvce.com □ is best website to obtain " SPLK-1002 " for free download □New Soft SPLK-1002 Simulations
- Get Valid Splunk SPLK-1002 Exam Questions and Answer □ Open ▸ www.exam4labs.com ◂ enter [SPLK-1002] and obtain a free download □Exam Cram SPLK-1002 Pdf
- Pass Guaranteed Quiz Authoritative Splunk - New SPLK-1002 Study Materials □ Open ➤ www.pdfvce.com □ enter ➡ SPLK-1002 □□□ and obtain a free download □SPLK-1002 Valid Exam Online
- New SPLK-1002 Study Materials has 100% pass rate, Splunk Core Certified Power User Exam □ Easily obtain " SPLK-1002 " for free download through ▹ www.dumpsquestion.com ◃ □Exam SPLK-1002 Vce
- church.ktcbcourses.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, hashnode.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, anonup.com, tastycraftacademy.com, www.stes.tyc.edu.tw, Disposable vapes

DOWNLOAD the newest Actualtests4sure SPLK-1002 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1W3O0YXhVe7N4ywD4MDirXG1IvWK3Dcdo