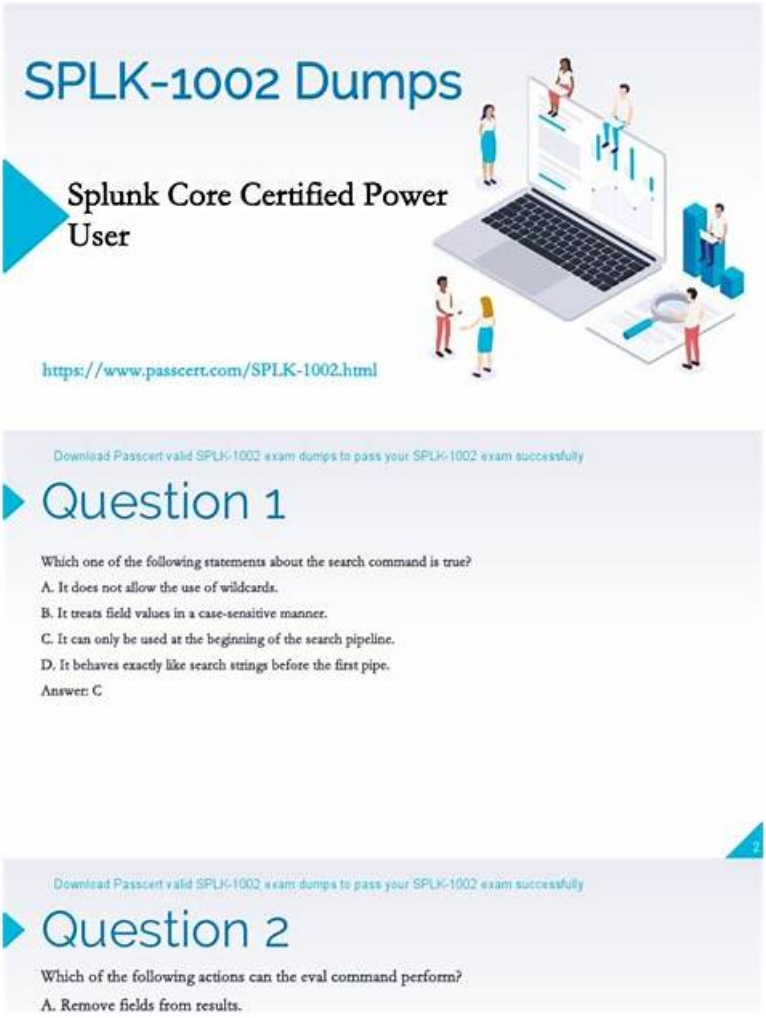
Make Exam Preparation Simple Splunk SPLK-1002 Exam Questions



BTW, DOWNLOAD part of PDF4Test SPLK-1002 dumps from Cloud Storage: https://drive.google.com/open?id=1kf2ZtP6WKwFMVu138UL20-TPflnpWfyr

The whole payment process on our SPLK-1002 exam braindumps only lasts a few seconds as long as there has money in your credit card. Then our system will soon deal with your orders according to the sequence of payment. Usually, you will receive the SPLK-1002 Study Materials no more than five minutes. Then you can begin your new learning journey of our SPLK-1002 praparation questions. All in all, our payment system and delivery system are highly efficient.

splk-1002 Exam topics

Candidates must know the exam topics before they start of preparation. Because it will really help them in hitting the core. Our **splk-1002 exam dumps** will include the following topics:

1. Splunk Fundamentals

- Refine searches
- Understand fields
- Installing Splunk
- Describe alerts

- Module 12 - Using Pivot
- Create a pivot report
- Identify the contents of search results
- Overview of Buttercup Games Inc.
- Learn basic navigation in Splunk
- Save search results
- Module 6 - Search Language Fundamentals
- Use fields in searches
- Review basic search commands and general search practices
- The stats command
- What is the Common Information Model (CIM)?
- The top command
- Understand the uses of Splunk
- Edit a dashboard
- Customizing your user settings
- Describe Pivot
- Use the fields sidebar
- Module 11 - Creating Scheduled Reports and Alerts
- Control a search job
- Use SPL search commands to perform searches:
- Module 4 - Basic Searching
- Add a report to a dashboard
- Understand the relationship between data models and pivot
- Work with events
- Create a dashboard
- Describe lookups
- Module 10 - Creating and Using Lookups
- Use autocomplete to help build a search
- The rare command
- Save a search as a report
- Describe scheduled reports
- Configure an automatic lookup
- Configure scheduled reports
- Create an instant pivot from a search

- Use the timeline
- Splunk components
- View fired alerts
- What are datasets?
- Create alerts
- Examine the search pipeline
- Getting data into Splunk
- Module 9 - Datasets and the Common Information Model
- Module 7 - Using Basic Transforming Commands
- Create reports that include visualizations such as charts
- Module 8 - Creating Reports and Dashboards
- Define Splunk Apps
- Use autocomplete and syntax highlighting
- Specify indexes in searches
- Set the time range of a search
- Add a pivot report to a dashboard
- Edit reports

2. Splunk Fundamentals

- Case sensitivity
- Add and use arguments with a macro
- Describe the Splunk CIM
- Module 8 - Creating and Managing Fields
- List the knowledge objects included with the Splunk CIM
- Perform delimiter field extractions using the FX
- Create and use a basic macro
- Lab environment
- Create a POST workflow action
- Create a GET workflow action
- Create a Search workflow action
- Explore data structure requirements
- Search fundamentals review
- Create a data model
- Module 4 - Using Mapping and Single Value Commands
- Module 1 - Introduction

- Review permissions
- Module 3 - Using Transforming Commands for Visualizations
- Perform regex field extractions using the Field Extractor (FX)
- Create and use tags
- Determine when to use transactions vs. stats
- Report on transactions
- Module 9 - Creating Field Aliases and Calculated Fields
- Add-On
- Module 12 - Creating and Using Workflow Actions
- Module 6 - Correlating Events
- Group events using fields
- Using the job inspector to view search performance
- Define arguments and variables for a macro
- Identify transactions
- Create and format charts and timecharts
- Describe event types and their uses
- The filnull command
- Module 7 - Introduction to Knowledge Objects
- Identify data model attributes
- Search with transactions
- Describe the function of GET, POST, and Search workflow actions
- Describe, create and use calculated fields
- The geostats command
- Describe macros
- Overview of Buttercup Games Inc.
- Module 2 - Beyond Search Fundamentals
- Group events using fields and time
- Manage knowledge objects
- Describe, create, and use field aliases
- Module 5 - Filtering and Formatting Results
- The eval command
- Module 10 - Creating Tags and Event Types
- Module 13 - Creating Data Models
- Use the CIM Add-On to normalize data

- Using the search and where commands to filter results
- The iplocation command
- The addtotals command

The SPLK-1002 Certification Exam is designed to test the advanced knowledge and skills of individuals who use Splunk on a regular basis. Splunk Core Certified Power User Exam certification is highly respected in the IT industry and is recognized by many employers as a validation of a candidate's expertise in Splunk. Earning this certification can open up new career opportunities and increase earning potential for individuals who work with Splunk.

To pass the Splunk SPLK-1002 exam, candidates must demonstrate a deep understanding of the Splunk platform and its various capabilities. SPLK-1002 exam is comprised of 65 multiple-choice and matching questions, and candidates have 90 minutes to complete it. Passing the exam requires a score of at least 70%, and successful candidates will receive the Splunk Core Certified Power User certification. Splunk Core Certified Power User Exam certification is highly regarded in the IT industry and can be a valuable asset for individuals seeking to advance their careers in IT operations, security, or data analytics.

100% Pass Quiz Splunk - SPLK-1002 - Splunk Core Certified Power User Exam Latest Training Tools

The Splunk SPLK-1002 exam questions are designed and verified by experienced and qualified Splunk SPLK-1002 exam trainers. So you rest assured that with Splunk Core Certified Power User Exam (SPLK-1002) exam dumps you can streamline your SPLK-1002 exam preparation process and get confidence to pass Splunk Core Certified Power User Exam (SPLK-1002) exam in first attempt.

Splunk Core Certified Power User Exam Sample Questions (Q164-Q169):

NEW QUESTION # 164
Based on the macro definition shown below, what is the correct way to execute the macro in a search string?

- A. 'convert_sales($euro$,$€$,$.79$)'
- B. "convert_sales(euro,€,.79)"
- C. "convert_sales($euro$,$€$,$.79$)"
- D. 'convert_sales(euro,€,.79)'

Answer: D

Explanation:
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Usesearchmacros

NEW QUESTION # 165
Which field extraction method should be selected for comma-separated data?

- A. Delimiters
- B. eval expression
- C. Regular expression
- D. table extraction

Answer: A

Explanation:
Explanation
The correct answer is B. Delimiters. This is because the delimiters method is designed for structured event data, such as data from files with headers, where all of the fields in the events are separated by a common delimiter, such as a comma or space. You can select a sample event, identify the delimiter, and then rename the fields that the field extractor finds. You can learn more about the delimiters method from the Splunk documentation1. The other options are incorrect because they are not suitable for comma-separated data. The regular expression method works best with unstructured event data, where you select and highlight one or more

fields to extract from a sample event, and the field extractor generates a regular expression that matches similar events and extracts the fields from them. The eval expression is a command that lets you calculate new fields or modify existing fields using arithmetic, string, and logical operations. The table extraction is a feature that lets you extract tabular data from PDF files or web pages. You can learn more about these methods from the Splunk documentation23 .

NEW QUESTION # 166
A calculated field maybe based on which of the following?

- A. Lookup tables
- B. Extracted fields
- C. Regular expressions
- D. Fields generated within a search string

Answer: B

Explanation:
As mentioned before, a calculated field is a field that you create based on the value of another field or fields2. A calculated field can be based on extracted fields, which are fields that are extracted from your raw data using various methods such as regular expressions, delimiters or key-value pairs2. Therefore, option B is correct, while options A, C and D are incorrect because they are not types of fields that a calculated field can be based on.

NEW QUESTION # 167
Which of the following searches will return events containing a tag named Privileged?

- A. tag=privileged
- B. tag=Priv*
- C. tag=Priv
- D. tag=priv*

Answer: A

Explanation:
Explanation/Reference: https://docs.splunk.com/Documentation/PCI/4.1.0/Install/PrivilegedUserActivity

NEW QUESTION # 168
How many ways are there to access the Field Extractor Utility?

- A. 0
- B. 1
- C. 2
- D. 3

Answer: C

NEW QUESTION # 169
.....

- Reliable SPLK-1002 Exam Simulations □ SPLK-1002 Torrent □ SPLK-1002 Exam Tips □ □ www.vce4dumps.com □ is best website to obtain ➡ SPLK-1002 □□□ for free download □Reliable SPLK-1002 Exam Book
- Real SPLK-1002 Exam Questions □ Instant SPLK-1002 Access ↗ Reliable SPLK-1002 Dumps Files □ Copy URL ✔ www.pdfvce.com □✔□ open and search for " SPLK-1002 " to download for free □Practice SPLK-1002 Tests
- Hot Training SPLK-1002 Tools Free PDF | Latest SPLK-1002 Certification Exam Infor: Splunk Core Certified Power User Exam ☯ Search for □ SPLK-1002 □ and obtain a free download on □ www.easy4engine.com □ □SPLK-1002 Test Questions Pdf
- Exam SPLK-1002 Blueprint □ Latest SPLK-1002 Exam Testking □ Reliable SPLK-1002 Exam Book □ Search for [SPLK-1002] and download it for free immediately on ⇛ www.pdfvce.com ⇚ □SPLK-1002 Valid Test Experience
- Practice SPLK-1002 Tests □ SPLK-1002 Valid Test Experience □ Instant SPLK-1002 Access □ Enter 【 www.easy4engine.com 】 and search for [SPLK-1002] to download for free □Practice SPLK-1002 Mock
- Training SPLK-1002 Tools 100% Pass | High-quality Splunk Core Certified Power User Exam Certification Exam Infor Pass for sure □ Search for ✔ SPLK-1002 □✔□ and easily obtain a free download on 《 www.pdfvce.com 》 □ □Practice SPLK-1002 Mock
- Real SPLK-1002 Exam Questions □ SPLK-1002 Torrent □ SPLK-1002 Exam Tips □ Download □ SPLK-1002 □ for free by simply searching on ⇛ www.examcollectionpass.com ⇚ □SPLK-1002 Latest Dumps Free
- SPLK-1002 Valid Test Experience □ Regualer SPLK-1002 Update □ SPLK-1002 Valid Test Experience □ Simply search for 《 SPLK-1002 》 for free download on ➽ www.pdfvce.com □ □SPLK-1002 Latest Torrent
- SPLK-1002 Test Torrent - SPLK-1002 Actual Test - SPLK-1002 Pass for Sure □ Go to website ➥ www.troytecdumps.com □ open and search for （ SPLK-1002 ） to download for free □Instant SPLK-1002 Access
- Hot Training SPLK-1002 Tools Free PDF | Latest SPLK-1002 Certification Exam Infor: Splunk Core Certified Power User Exam □ Simply search for □ SPLK-1002 □ for free download on ☀ www.pdfvce.com □☀□ □Reliable SPLK-1002 Dumps Files
- SPLK-1002 Test Questions Pdf □ SPLK-1002 Valid Test Experience □ Instant SPLK-1002 Access □ Enter ▸ www.examcollectionpass.com ◂ and search for ⇛ SPLK-1002 ⇚ to download for free □Real SPLK-1002 Exam Questions
- pr7bookmark.com, www.stes.tyc.edu.tw, schoolido.lu, larabzbb882633.bcbloggers.com, hhi.instructure.com, tetrabookmarks.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, 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, Disposable vapes

BTW, DOWNLOAD part of PDF4Test SPLK-1002 dumps from Cloud Storage: https://drive.google.com/open?id=1kf2ZtP6WKwFMVu138UL20-TPflnpWfyr