Splunk SPLK-1002

Splunk Core Power User Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

SPLK-1002

Splunk Core Certified Power User

57 Questions Exam – 700 / 1000 Cut Score – Duration of 65 minutes

Table of Contents:

Discover More about the Splunk SPLK-1002 Certification

Are you interested in passing the Splunk SPLK-1002 exam? First discover, who benefits from the SPLK-1002 certification. The SPLK-1002 is suitable for a candidate if he wants to learn about Core. Passing the SPLK-1002 exam earns you the Splunk Core Certified Power User title.

While preparing for the SPLK-1002 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The SPLK-1002 PDF contains some of the most valuable preparation tips and the details and instant access to useful **SPLK-1002 study materials just at one click.**

Splunk SPLK-1002 Core Power User Certification Details:

Exam Name	Splunk Core Certified Power User
Exam Code	SPLK-1002
Exam Price	$130 (USD)
Duration	65 mins
Number of Questions	57
Passing Score	**700 / 1000**
Schedule Exam	**Pearson VUE**
Sample Questions	**Splunk Core Power User Sample Questions**
Practice Exam	**Splunk SPLK-1002 Certification Practice Exam**

Splunk SPLK-1002 Syllabus:

Topic	**Details**	**Weights**
Using Transforming Commands for Visualizations	- Use the chart command - Use the timechart command	5%
Filtering and Formatting Results	- The eval command - Use the search and where commands to filter results - The fillnull command	10%
Correlating Events	- Identify transactions - Group events using fields	15%

Topic	Details	Weights
	- Group events using fields and time - Search with transactions - Report on transactions - Determine when to use transactions vs. stats	
Creating and Managing Fields	- Perform regex field extractions using the Field Extractor (FX) - Perform delimiter field extractions using the FX	10%
Creating Field Aliases and Calculated Fields	- Describe, create, and use field aliases - Describe, create, and use calculated fields	10%
Creating Tags and Event Types	- Create and use tags - Describe event types and their uses - Create an event type	10%
Creating and Using Macros	- Describe macros - Create and use a basic macro - Define arguments and variables for a macro - Add and use arguments with a macro	10%
Creating and Using Workflow Actions	- Describe the function of GET, POST, and Search workflow actions - Create a GET workflow action - Create a POST workflow action - Create a Search workflow action	10%
Creating Data Models	- Describe the relationship between data models and pivot - Identify data model attributes - Create a data model	10%
Using the Common Information Model (CIM) Add-On	- Describe the Splunk CIM - List the knowledge objects included with the Splunk CIM Add-On - Use the CIM Add-On to normalize data	10%

Broaden Your Knowledge with Splunk SPLK-1002 Sample Questions:

Question: 1

Which of the following statements would help a user choose between the transaction and stats commands?

a) stats can only group events using IP addresses.
b) The transaction command is faster and more efficient.
c) There is a 1000 event limitation with the transaction command.
d) Use stats when the events need to be viewed as a single correlated event.

Answer: c

Question: 2

What is the correct syntax to search for a tag associated with a value on a specific field?

a) tag=<field>
b) tag=<field>(<tagname>)
c) tag=<field>::<tagname>
d) tag::<field>=<tagname>

Answer: d

Question: 3

When creating a Search workflow action, which field is required?

a) Search string
b) Data model name
c) Permission setting
d) An eval statement

Answer: a

Question: 4

What are the two parts of a root event dataset?

a) Fields and variables.
b) Fields and attributes.
c) Constraints and fields.
d) Constraints and lookups.

Answer: c

Question: 5

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? (Choose all that apply.)

a) Fast mode is enabled.
b) The dashboard is private.
c) The extraction is private.
d) The person in the organization running the report does not have access to the index.

Answer: c, d

Question: 6

Calculated fields can be based on which of the following?

a) Tags
b) Extracted fields
c) Output fields for a lookup
d) Fields generated from a search string

Answer: b

Question: 7

Which workflow uses field values to perform a secondary search?

a) Search
b) POST
c) Action
d) Sub-search

Answer: a

Question: 8

In most large Splunk environments, what is the most efficient command that can be used to group events by fields?

a) join
b) stats
c) streamstats
d) transaction

Answer: b

Question: 9

Which of the following knowledge objects represents the output of an eval expression?

a) Calculated fields
b) Field extractions
c) Eval fields
d) Calculated lookups

Answer: a

Question: 10

A data model can consist of what three types of datasets?

a) Pivot, events, and transactions.
b) Searches, transactions, and pivot.
c) Pivot, searches, and events.
d) Events, searches, and transactions.

Answer: d

Avail the Study Guide to Pass Splunk SPLK-1002 Core Power User Exam:

- Find out about the SPLK-1002 syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **Splunk SPLK-1002 syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.
- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the **Core Power User training.** Joining the Splunk provided training for this Splunk certification exam helps a candidate to strengthen his practical knowledge base from the certification.

- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **Splunk SPLK-1002 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. SPLK-1002 practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

Passing the Splunk SPLK-1002 exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.