Splunk SPLK-1004

Splunk Core Advanced Power User Certification Questions & Answers

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

SPLK-1004

Splunk Core Certified Advanced Power User

70 Questions Exam – 700/1000 Cut Score – Duration of 60 minutes

Table of Contents:

Discover More about the Splunk SPLK-1004 Certification

Are you interested in passing the Splunk SPLK-1004 exam? First discover, who benefits from the SPLK-1004 certification. The SPLK-1004 is suitable for a candidate if he wants to learn about Core. Passing the SPLK-1004 exam earns you the Splunk Core Certified Advanced Power User title.

While preparing for the SPLK-1004 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The SPLK-1004 PDF contains some of the most valuable preparation tips and the details and instant access to useful **SPLK-1004 study materials just at one click.**

Splunk SPLK-1004 Core Advanced Power User Certification Details:

Exam Name	Splunk Core Certified Advanced Power User
Exam Code	SPLK-1004
Exam Price	$130 (USD)
Duration	60 mins
Number of Questions	70
Passing Score	700/1000
Schedule Exam	**Pearson VUE**
Sample Questions	**Splunk Core Advanced Power User Sample Questions**
Practice Exam	**Splunk SPLK-1004 Certification Practice Exam**

Splunk SPLK-1004 Syllabus:

Topic	Details	Weights
Exploring Statistical Commands	- Performing statistical analysis with stats function - Using fieldsummary - Using appendpipe - Using count and list functions - Using eventstats - Using streamstats	4%

Topic	Details	Weights
Exploring eval Command Functions	- Using conversion functions - Using text functions - Using comparison and conditional functions - Using informational functions - Using statistical functions - Using makeresults command	4%
Exploring Lookups	- Applying advanced lookup options - Including and excluding events based on lookup values - Using KV Store lookups - Using external lookups - Using geospatial lookups - Understanding best practices for lookups	4%
Exploring Alerts	- Logging and indexing searchable alert events - Referencing lookups in alerts - Outputting alert results to a lookup - Using a webhook alert action - Creating a log event alert action	4%
Advanced Field Creation and Management	- Identifying field extraction methods - Providing a regex expression to the Field Extractor to extract a field - Performing search time field extraction using the erex and rex commands - Understand how to improve regex performance in Splunk	4%
Working with Self-Describing Data and Files	- Understanding self-describing data - Using the spath command - Using the eval command with the spath function - Using the multikv command	3%
Advanced Search Macros	- Using nested search macros - Previewing search macros before executing - Using other knowledge objects with macros	3%
Using Acceleration Options: Reports and Summary Indexing	- Describing acceleration - Identifying which reports qualify for acceleration - Identifying when Splunk doesn’t build an acceleration summary - Accelerating a report	4%

Topic	Details	Weights
	- Using the Report Acceleration Summaries and Summary Detail pages - Understanding summary Indexing - Using the summary indexing transforming commands - Defining searching against a summary - Understanding how to handle gaps and overlaps in summary indexes	
Using Acceleration Options: Data Models and tsidx Files	- Exploring data models using the datamodel command - Understanding data model acceleration - Accelerating data models - Understanding tsidx files - Working with tsidx files using tstats commands - Using tstats to search accelerated data models - Determining which acceleration option to use	4%
Using Search Efficiently	- Splunk architecture components - Search flow - Streaming commands - Transforming commands - Command ordering - Job inspector	4%
More Search Tuning	- Pre-Filtering search data - Lispy and boolean operators - Lispy and wildcards - Using the TERM directive	3%
Manipulating and FIltering Data	- bin command - xyseries command - untable command - foreach command - strftime function	6%
Working with Multivalued Fields	- Multivalued fields - Some multivalued eval functions - makemv command - mvexpand command	7%
Using Advanced Transactions	- Evaluating events to create transactions - Handling common values/different field names - An alternative to coalesce	5%

Topic	Details	Weights
	- Identifying complete vs. incomplete transactions - Making transactions more efficient - stats and transactions	
Working with Time	- Using time effectively - What are the default time fields	2%
Using Subsearches	- Filtering through many results - Subsearch caveats - When to use subsearch - When NOT to use subsearch - Troubleshooting subsearches - append command	6%
Creating a Prototype	- Define simple XML syntax for views - Use best practices for creating views - Troubleshooting views	4%
Using Forms	- Explain how tokens work - Use tokens with form inputs - Create cascading inputs - Define types of token filters	5%
Improving Performance	- Identify ways to improve dashboard performance - Use the tstats command - Create base and post-process searches	6%
Customizing Dashboards	- Customize chart and panel properties - Set panel refresh and delay times - Disable search access features - Create event annotations	6%
Adding Drilldowns	- Define types of drilldowns - Identify predefined tokens - Create dynamic drilldowns	7%
Adding Advanced Behaviors and Visualizations	- Identify types of event handlers - Define event actions - Create contextual drilldowns	5%

Broaden Your Knowledge with Splunk SPLK-1004 Sample Questions:

Question: 1

Which factors are crucial in creating effective event handlers in a dashboard? (Choose two)

a) Ensuring that handlers are unrelated to user actions.
b) Designing handlers to respond to specific user interactions.
c) Creating handlers that enhance user experience and data analysis.
d) Implementing handlers that reduce dashboard functionality.

Answer: b, c

Question: 2

What are the purposes of using streamstats in Splunk searches? (choose two)

a) To perform transformations on streaming data
b) To calculate running totals or averages
c) To filter streaming data
d) To aggregate data based on a time window

Answer: b, d

Question: 3

The eval command is primarily used for which purpose?

a) Filtering data
b) Creating or modifying fields
c) Generating alerts
d) Creating lookups

Answer: b

Question: 4

How do tokens in dashboard design improve user experience?

a) By increasing load times.
b) By allowing dynamic content updates.
c) By limiting user interaction.
d) By reducing customization options.

Answer: b

Question: 5

What are the purposes of using streamstats in Splunk searches?

(choose two)

a) To perform transformations on streaming data
b) To calculate running totals or averages
c) To filter streaming data
d) To aggregate data based on a time window

Answer: b, d

Question: 6

Which of these are multivalued eval functions in Splunk?

(Choose two)

a) mvjoin
b) mvexpand
c) mvcount
d) mvindex

Answer: c, d

Question: 7

In customizing chart properties, which aspects are important to consider?

(Choose two)

a) Uniform color schemes regardless of data.
b) Data readability and visualization clarity.
c) Using complex chart types for simple data.
d) Matching chart types with data nature.

Answer: b, d

Question: 8

When dealing with multivalued fields, mvexpand is used to:

a) Join multiple values into a single string
b) Create a new event for each value of a multivalued field
c) Count the number of values in a field
d) Extract values from a structured data field

Answer: b

Question: 9

In advanced dashboard design, how are dynamic drilldowns typically implemented?

a) By using hard-coded links.
b) Through static text displays.
c) By utilizing predefined tokens and user interaction data.
d) By avoiding any form of user interaction.

Answer: c

Question: 10

How can you split a single-valued field into multiple values?

a) Using the split command
b) Applying the mvexpand command
c) Using the eval command with a separator
d) Applying the multisplit function

Answer: b

Avail the Study Guide to Pass Splunk SPLK-1004 Core Advanced Power User Exam:

- Find out about the SPLK-1004 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-1004 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 Advanced 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-1004 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. SPLK-1004 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-1004 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.