certfun.com
#1 IT Certification Guide

Splunk SPLK-1001

Splunk Core User Certification Questions & Answers

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

SPLK-1001

Splunk Core Certified User

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

Table of Contents:

Discover More about the Splunk SPLK-1001 Certification 2

Splunk SPLK-1001 Core User Certification Details: 2

Splunk SPLK-1001 Syllabus:....................................... 2

Broaden Your Knowledge with Splunk SPLK-1001 Sample Questions: 4

Avail the Study Guide to Pass Splunk SPLK-1001 Core User Exam:.. 6

Career Benefits: 7

Discover More about the Splunk SPLK-1001 Certification

Are you interested in passing the Splunk SPLK-1001 exam? First discover, who benefits from the SPLK-1001 certification. The SPLK-1001 is suitable for a candidate if he wants to learn about Core. Passing the SPLK-1001 exam earns you the Splunk Core Certified User title.

While preparing for the SPLK-1001 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The SPLK-1001 PDF contains some of the most valuable preparation tips and the details and instant access to useful **SPLK-1001 study materials just at one click.**

Splunk SPLK-1001 Core User Certification Details:

Exam Name	Splunk Core Certified User
Exam Code	SPLK-1001
Exam Price	$130 (USD)
Duration	60 mins
Number of Questions	60
Passing Score	700 / 1000
Schedule Exam	**Pearson VUE**
Sample Questions	**Splunk Core User Sample Questions**
Practice Exam	**Splunk SPLK-1001 Certification Practice Exam**

Splunk SPLK-1001 Syllabus:

Topic	**Details**	**Weights**
Splunk Basics	- Splunk components - Understand the uses of Splunk - Define Splunk apps - Customizing user settings - Basic navigation in Splunk	5%
Basic Searching	- Run basic searches - Set the time range of a search - Identify the contents of search results - Refine searches - Use the timeline	22%

Topic	Details	Weights
	- Work with events - Control a search job - Save search results	
Using Fields in Searches	- Understand fields - Use fields in searches - Use the fields sidebar	20%
Search Language Fundamentals	- Review basic search commands and general search practices - Examine the search pipeline - Specify indexes in searches - Use the following commands to perform searches: tables, rename, fields, dedup, and sort	15%
Using Basic Transforming Commands	- The top command - The rare command - The stats command	15%
Creating Reports and Dashboards	- Save a search as a report - Edit reports - Create reports that display statistics (tables) - Create reports that display visualizations (charts) - Create a dashboard - Add a report to a dashboard - Edit a dashboard	12%
Creating and Using Lookups	- Describe lookups - Examine a lookup file example - Create a lookup file and create a lookup definition - Configure an automatic lookup - Use the lookup in searches	6%
Creating Scheduled Reports and Alerts	- Describe scheduled reports - Configure scheduled reports - Describe alerts - Create alerts - View fired alerts	5%

Broaden Your Knowledge with Splunk SPLK-1001 Sample Questions:

Question: 1

Which of the following constraints can be used with the top command?

a) useperc
b) limit
c) addtotals
d) fieldcount

Answer: b

Question: 2

What does the stats command do?

a) Automatically correlates related fields.
b) Converts field values into numerical values.
c) Calculates statistics on data that matches the search criteria.
d) Analyzes numerical fields for their ability to predict another discrete field.

Answer: c

Question: 3

When running searches, command modifiers in the search string are displayed in what color?

a) Red
b) Orange
c) Blue
d) Highlighted

Answer: b

Question: 4

In the Splunk interface, the list of alerts can be filtered based on which characteristics?

a) App, Owner, Priority, and Status
b) App, Dashboard, Severity, and Type
c) App, Owner, Severity, and Type
d) App, Time Window, Type, and Severity

Answer: c

Question: 5

Splunk index time process can be broken down into __________ phases.

a) 2
b) 3
c) 4
d) 1

Answer: b

Question: 6

How can another user gain access to a saved report?

a) The owner of the report can edit permissions from the Edit dropdown.
b) Only users with an Admin or Power User role can access other users' reports.
c) Anyone can access any reports marked as public within a shared Splunk deployment.
d) The owner of the report must clone the original report and save it to their user account.

Answer: a

Question: 7

Log filtering/parsing can be done from ____________.

a) Index Forwarders (IF)
b) Universal Forwarders (UF)
c) Super Forwarder (SF)
d) Heavy Forwarders (HF)

Answer: d

Question: 8

Which of the following represents the Splunk recommended naming convention for dashboards?

a) Description_Group_Object
b) Group_Description_Object
c) Group_Object_Description
d) Object_Group_Description

Answer: c

Question: 9

How can search results be kept longer than 7 days?

a) By scheduling a report.
b) By creating a link to the job.
c) By changing the job settings.
d) By changing the time range picker to more than 7 days.

Answer: a

Question: 10

By default, which of the following is a Selected Field?

a) action
b) clientip
c) categoryId
d) sourcetype

Answer: d

Avail the Study Guide to Pass Splunk SPLK-1001 Core User Exam:

- Find out about the SPLK-1001 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-1001 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 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-1001 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. SPLK-1001 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-1001 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.

Here Is the Trusted Practice Test for the Splunk SPLK-1001 Certification

CertFun.Com is here with all the necessary details regarding the SPLK-1001 exam. We provide authentic practice tests for the SPLK-1001 exam. What do you gain from these practice tests? You get to experience the real exam-like questions made by industry experts and get a scope to improve your performance in the actual exam. Rely on CertFun.Com for rigorous, unlimited two-month attempts on the **SPLK-1001 practice tests**, and gradually build your confidence. Rigorous practice made many aspirants successful and made their journey easy towards grabbing the Splunk Core Certified User.

Start Online practice of Splunk SPLK-1001 Exam by visiting URL
https://www.certfun.com/splunk/splk-1001-splunk-core-certified-user