certfun.com
#1 IT Certification Guide

SPLUNK SPLK-1003 STUDY GUIDE PDF

Grab the Splunk Enterprise Admin Certification PDF Questions & Answers

Details of the Exam-Syllabus-Questions

SPLK-1003

Splunk Enterprise Certified Administrator

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

www.CertFun.com

Table of Contents:

Get an Overview of the SPLK-1003 Certification:

Who should take the **SPLK-1003 exam**? This is the first question that comes to a candidate’s mind when preparing for the Enterprise Admin certification. The SPLK-1003 certification is suitable for candidates who are keen to earn knowledge on the Enterprise and grab their Splunk Enterprise Certified Administrator. When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But SPLK-1003 study guide PDF is here to solve the problem. SPLK-1003 PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the Splunk SPLK-1003 Certification?

There are several reasons why one should grab the SPLK-1003 certification.

- The Enterprise Admin certification proves to be one of the most recognized certifications.
- The certification badge proves the knowledge of the candidate regarding subject matters and makes his resume presentable to potential candidates.
- Thus earning the **Splunk Enterprise Certified Administrator** is a powerful qualification for a prosperous career.

What Is the Splunk SPLK-1003 Enterprise Admin Certification Exam Structure?

Exam Name	Splunk Enterprise Certified Administrator
Exam Code	SPLK-1003
Exam Price	$130 (USD)
Duration	60 mins
Number of Questions	56
Passing Score	700 / 1000
Schedule Exam	**Pearson VUE**
Sample Questions	**Splunk Enterprise Admin Sample Questions**
Practice Exam	**Splunk SPLK-1003 Certification Practice Exam**

Enhance Knowledge with SPLK-1003 Sample Questions:

Question: 1

You update a props.conf file while Splunk is running. You do not restart Splunk and you run this command: splunk btool props list –-debug. What will the output be?

a) A list of all the configurations on-disk that Splunk contains.
b) A verbose list of all configurations as they were when splunkd started.
c) A list of props.conf configurations as they are on-disk along with a file path from which the configuration is located.
d) A list of the current running props.conf configurations along with a file path from which the configuration was made.

Answer: c

Question: 2

Consider a company with a Splunk distributed environment in production. The Compliance Department wants to start using Splunk; however, they want to ensure that no one can see their reports or any other knowledge objects.

Which Splunk Component can be added to implement this policy for the new team?

a) Indexer
b) Deployment server
c) Universal forwarder
d) Search head

Answer: d

Question: 3

If an update is made to an attribute in inputs.conf on a universal forwarder, on which Splunk component would the fishbucket need to be reset in order to reindex the data?

a) Indexer
b) Search head
c) Deployment server
d) Forwarder

Answer: d

Question: 4

Which Splunk component receives, indexes, and stores incoming data from forwarders?

a) Indexer
b) Search head
c) Cluster master
d) Deployment server

Answer: a

Question: 5

Which license type allows 500MB/day of indexing, but disables alerts, authentication, cluster, distributed search, summarization, and forwarding to non-Splunk servers?

a) Free license
b) Forwarder license
c) Enterprise license
d) Enterprise trial license

Answer: a

Question: 6

For single line event sourcetypes, it is most efficient to set SHOULD_LINEMERGE to what value?

a) True
b) False
c) regex string
d) Newline Character

Answer: b

Question: 7

How can native authentication be disabled in Splunk?

a) Create an empty $SPLUNK_HOME/etc/passwd file
b) Remove the $SPLUNK_HOME/etc/passwd file
c) Set SPLUNK_AUTHENTICATION=false in splunk-launch.conf
d) Set nativeAuthentication=false in authentication.conf

Answer: a

Question: 8

To set up a network input in Splunk, what needs to be specified?

a) File path.
b) Username and password.
c) Network protocol and port number.
d) Network protocol and MAC address.

Answer: c

Question: 9

An organization wants to collect Windows performance data from a set of clients, however, installing Splunk software on these clients is not allowed. What option is available to collect this data in Splunk Enterprise?

a) Use Local Windows host monitoring.
b) Use Windows Remote Inputs with WMI.
c) Use Local Windows network monitoring.
d) Use an index with an Index Data Type of Metrics.

Answer: b

Question: 10

What can be used when setting the host field option on a network input?

(select all that apply)

a) IP
b) DNS
c) A binary file
d) Custom (explicit value)

Answer: a, b, d

What Study Guide Works Best in Acing the Splunk SPLK-1003 Enterprise Admin Certification?

The SPLK-1003 study guide is a combination of some proven study tips and the combination of all valuable study materials like sample questions, syllabus and practice tests in one place.

Explore the Syllabus Topics and Learn from the Core:

If you are determined to earn success in the Enterprise Admin exam, getting in full touch of the **syllabus** is mandatory. During preparation, you might not like all syllabus sections or topics, but try to get at least the fundamental knowledge from the sections you don't like. The more you possess knowledge on all syllabus sections, the more is the chance to attempt maximum number of questions during the actual exam.

Make Your Schedule:

Studying and completing the syllabus becomes easier, if you work on the syllabus topics after making a schedule. Your syllabus must mention what areas you want to cover and within what time. Once you make a schedule and follow it regularly, syllabus completion becomes easier and preparation becomes smoother.

Get Expert Advice from the Training:

Do not forget to join the Splunk SPLK-1003 training if it is providing any. Training enhances the practical knowledge of a candidate, which helps them to work well in the practical field during projects.

Get Access to the PDF Sample Questions:

If your study material is in a **PDF format** or the materials are mobile-friendly, what could be better than that? Get access to the free sample questions and keep enhancing your knowledge beyond the syllabus.

Avoid Dumps and Utilize the Splunk SPLK-1003 Practice Test:

Why should you rely on practice tests? The reason is simple: you must get familiar with the exam pattern before reaching the exam hall. An aspirant aware of the exam structure and time management during the exam preparation can perform well in the actual exam and attempt the maximum number of questions during the exam.

Many aspirants prefer to read from dumps, but they miss out on the self assessment method. Therefore, SPLK-1003 practice tests always stand out to be the better choice than dumps PDF.