Splunk SPLK-1003

Splunk Enterprise Admin Certification Questions & Answers

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

SPLK-1003

Splunk Enterprise Certified Administrator

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

Table of Contents:

Discover More about the Splunk SPLK-1003 Certification

Are you interested in passing the Splunk SPLK-1003 exam? First discover, who benefits from the SPLK-1003 certification. The SPLK-1003 is suitable for a candidate if he wants to learn about Enterprise. Passing the SPLK-1003 exam earns you the Splunk Enterprise Certified Administrator title.

While preparing for the SPLK-1003 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The SPLK-1003 PDF contains some of the most valuable preparation tips and the details and instant access to useful **SPLK-1003 study materials just at one click**.

Splunk SPLK-1003 Enterprise Admin Certification Details:

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
Books / Training	**Splunk Enterprise System Administration** **Splunk Enterprise Data Administration**
Schedule Exam	**Pearson VUE**
Sample Questions	**Splunk Enterprise Admin Sample Questions**
Practice Exam	**Splunk SPLK-1003 Certification Practice Exam**

Splunk SPLK-1003 Syllabus:

Topic	**Details**	**Weights**
Splunk Admin Basics	- Identify Splunk components	5%
License Management	- Identify license types - Understand license violations	5%
Splunk Configuration Files	- Describe Splunk configuration directory structure - Understand configuration layering - Understand configuration precedence	5%

Topic	Details	Weights
	- Use btool to examine configuration settings	
Splunk Indexes	- Describe index structure - List types of index buckets - Check index data integrity - Describe indexes.conf options - Describe the fishbucket - Apply a data retention policy	10%
Splunk User Management	- Describe user roles in Splunk - Create a custom role - Add Splunk users	5%
Splunk Authentication Management	- Integrate Splunk with LDAP - List other user authentication options - Describe the steps to enable Multifactor Authentication in Splunk	5%
Getting Data In	- Describe the basic settings for an input - List Splunk forwarder types - Configure the forwarder - Add an input to UF using CL	5%
Distributed Search	- Describe how distributed search works - Explain the roles of the search head and search peers - Configure a distributed search group - List search head scaling options	10%
Getting Data In - Staging	- List the three phases of the Splunk Indexing process - List Splunk input options	5%
Configuring Forwarders	- Configure Forwarders - Identify additional Forwarder options	5%
Forwarder Management	- Explain the use of Deployment Management - Describe Splunk Deployment Server - Manage forwarders using deployment apps - Configure deployment clients - Configure client groups - Monitor forwarder management activities	10%
Monitor Inputs	- Create file and directory monitor inputs - Use optional settings for monitor inputs - Deploy a remote monitor input	5%
Network and Scripted Inputs	- Create network (TCP and UDP) inputs - Describe optional settings for network	5%

Topic	Details	Weights
	inputs - Create a basic scripted input	
Agentless Inputs	- Identify Windows input types and uses - Describe HTTP Event Collector	5%
Fine Tuning Inputs	- Understand the default processing that occurs during input phase - Configure input phase options, such as sourcetype fine-tuning and character set encoding	5%
Parsing Phase and Data	- Understand the default processing that occurs during parsing - Optimize and configure event line breaking - Explain how timestamps and time zones are extracted or assigned to events - Use Data Preview to validate event creation during the parsing phase	5%
Manipulating Raw Data	- Explain how data transformations are defined and invoked - Use transformations with props.conf and transforms.conf to: • Mask or delete raw data as it is being indexed • Override sourcetype or host based upon event values • Route events to specific indexes based on event content • Prevent unwanted events from being indexed - Use SEDCMD to modify raw data	5%

Broaden Your Knowledge with Splunk 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

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: 4

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

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

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: 7

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: 8

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: 9

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: 10

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

Avail the Study Guide to Pass Splunk SPLK-1003 Enterprise Admin Exam:

- Find out about the SPLK-1003 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-1003 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 **Enterprise Admin 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-1003 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. SPLK-1003 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-1003 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-1003 Certification

CertFun.Com is here with all the necessary details regarding the SPLK-1003 exam. We provide authentic practice tests for the SPLK-1003 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-1003 practice tests**, and gradually build your confidence. Rigorous practice made many aspirants successful and made their journey easy towards grabbing the Splunk Enterprise Certified Administrator.

Start Online practice of Splunk SPLK-1003 Exam by visiting URL https://www.certfun.com/splunk/splk-1003-splunk-enterprise-certified-admin