SPLUNK SPLK-3003 STUDY GUIDE PDF

Grab the Splunk Core Consultant Certification PDF Questions & Answers

Details of the Exam-Syllabus-Questions

SPLK-3003

Splunk Core Certified Consultant

86 Questions Exam – 700 / 1000 Cut Score – Duration of 120 minutes

www.CertFun.com

Table of Contents:

Get an Overview of the SPLK-3003 Certification:

Who should take the **SPLK-3003 exam**? This is the first question that comes to a candidate's mind when preparing for the Core Consultant certification. The SPLK-3003 certification is suitable for candidates who are keen to earn knowledge on the Core and grab their Splunk Core Certified Consultant. When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But SPLK-3003 study guide PDF is here to solve the problem. SPLK-3003 PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the Splunk SPLK-3003 Certification?

There are several reasons why one should grab the SPLK-3003 certification.

- The Core Consultant 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 Core Certified Consultant** is a powerful qualification for a prosperous career.

What Is the Splunk SPLK-3003 Core Consultant Certification Exam Structure?

Exam Name	Splunk Core Certified Consultant
Exam Code	SPLK-3003
Exam Price	$130 (USD)
Duration	120 mins
Number of Questions	86
Passing Score	700 / 1000
Schedule Exam	**Pearson VUE**
Sample Questions	**Splunk Core Consultant Sample Questions**
Practice Exam	**Splunk SPLK-3003 Certification Practice Exam**

Enhance Knowledge with SPLK-3003 Sample Questions:

Question: 1

In a large cloud customer environment with many (>100) dynamically created endpoint systems, each with a UF already deployed, what is the best approach for associating these systems with an appropriate serverclass on the deployment server?

a) Work with the cloud orchestration team to create a common host-naming convention for these systems so a simple pattern can be used in the serverclass.conf whitelist attribute.
b) Create a CSV lookup file for each severclass, manually keep track of the endpoints within this CSV file, and leverage the whitelist.from_pathname attribute in serverclass.conf.
c) Work with the cloud orchestration team to dynamically insert an appropriate clientName setting into each endpoint's local/deploymentclient.conf which can be matched by whitelist in serverclass.conf.
d) Using an installation bootstrap script run a CLI command to assign a clientName setting and permit serverclass.conf whitelist simplification.

Answer: c

Question: 2

When monitoring and forwarding events collected from a file containing unstructured textual events, what is the difference in the Splunk2Splunk payload traffic sent between a universal forwarder (UF) and indexer compared to the Splunk2Splunk payload sent between a heavy forwarder (HF) and the indexer layer?
(Assume that the file is being monitored locally on the forwarder.)

a) The payload format sent from the UF versus the HF is exactly the same. The payload size is identical because they're both sending 64K chunks.
b) The UF will generally send the payload in the same format, but only when the sourcetype is specified in the inputs.conf and EVENT_BREAKER_ENABLE is set to true.
c) The HF sends a stream of 64K TCP chunks with one set of metadata fields attached to represent the entire stream, whereas the UF sends individual events, each with their own metadata fields attached.
d) The UF sends a stream of data containing one set of medata fields to represent the entire stream, whereas the HF sends individual events, each with their own metadata fields attached, resulting in a lager payload.

Answer: d

Question: 3

A customer has 30 indexers in an indexer cluster configuration and two search heads. They are working on writing SPL search for a particular use-case, but are concerned that it takes too long to run for short time durations.

How can the Search Job Inspector capabilities be used to help validate and understand the customer concerns?

a) Search Job Inspector provides statistics to show how much time and the number of events each indexer has processed.
b) Search Job Inspector provides a Search Health Check capability that provides an optimized SPL query the customer should try instead.
c) Search Job Inspector cannot be used to help troubleshoot the slow performing search; customer should review index=_introspection instead.
d) The customer is using the transaction SPL search command, which is known to be slow.

Answer: a

Question: 4

A non-ES customer has a concern about data availability during a disaster recovery event. Which of the following Splunk Validated Architectures (SVAs) would be recommended for that use case?

a) Topology Category Code: M4
b) Topology Category Code: M14
c) Topology Category Code: C13
d) Topology Category Code: C3

Answer: a

Question: 5

Which event processing pipeline contains the regex replacement processor that would be called upon to run event masking routines on events as they are ingested?

a) Merging pipeline
b) Typing pipeline
c) Indexing pipeline
d) Parsing pipeline

Answer: b

Question: 6

A customer has three users and is planning to ingest 250GB of data per day. They are concerned with search uptime, can tolerate up to a two-hour downtime for the search tier, and want advice on single search head versus a search head cluster (SHC).
Which recommendation is the most appropriate?

a) The customer should deploy two active search heads behind a load balancer to support HA.
b) The customer should deploy a SHC with a single member for HA; more members can be added later.
c) The customer should deploy a SHC, because it will be required to support the high volume of data.
d) The customer should deploy a single search head with a warm standby search head and an rsync process to synchronize configurations.

Answer: d

Question: 7

The Splunk Validated Architectures (SVAs) document provides a series of approved Splunk topologies. Which statement accurately describes how it should be used by a customer?

a) Customer should look at the category tables, pick the highest number that their budget permits, then select this design topology as the chosen design.
b) Customers should identify their requirements, provisionally choose an approved design that meets them, then consider design principles and best practices to come to an informed design decision.
c) Using the guided requirements gathering in the SVAs document, choose a topology that suits requirements, and be sure not to deviate from the specified design.
d) Choose an SVA topology code that includes Search Head and Indexer Clustering because it offers the highest level of resilience.

Answer: b

Question: 8

Which of the following server roles should be configured for a host which indexes its internal logs locally?

a) Cluster master
b) Indexer
c) Monitoring Console (MC)
d) Search head

Answer: b

Question: 9

When utilizing a subsearch within a Splunk SPL search query, which of the following statements is accurate?

a) Subsearches have to be initiated with the | subsearch command.
b) Subsearches can only be utilized with | inputlookup command.
c) Subsearches have a default result output limit of 10000.
d) There are no specific limitations when using subsearches.

Answer: c

Question: 10

In addition to the normal responsibilities of a search head cluster captain, which of the following is a default behavior?

a) The captain is not a cluster member and does not perform normal search activities.
b) The captain is a cluster member who performs normal search activities.
c) The captain is not a cluster member but does perform normal search activities.
d) The captain is a cluster member but does not perform normal search activities.

Answer: b

What Study Guide Works Best in Acing the Splunk SPLK-3003 Core Consultant Certification?

The SPLK-3003 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 Core Consultant 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-3003 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-3003 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-3003 practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven SPLK-3003 Practice Test for Success!!!

Do you want to pass the SPLK-3003 exam on your first attempt? Stop worrying; we, CertFun.com are here to provide you the best experience during your Splunk Core Certified Consultant preparation. Try out our free mock tests to get a glimpse of our quality study materials, and build your confidence with the premium **SPLK-3003 practice tests**. Our expert-designed questions help you to improve performance and pass the exam on your first attempt.