Splunk SPLK-3003

Splunk Core Consultant Certification Questions & Answers

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

SPLK-3003

Splunk Core Certified Consultant

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

Table of Contents:

Discover More about the Splunk SPLK-3003 Certification

Are you interested in passing the Splunk SPLK-3003 exam? First discover, who benefits from the SPLK-3003 certification. The SPLK-3003 is suitable for a candidate if he wants to learn about Core. Passing the SPLK-3003 exam earns you the Splunk Core Certified Consultant title.

While preparing for the SPLK-3003 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The SPLK-3003 PDF contains some of the most valuable preparation tips and the details and instant access to useful **SPLK-3003 study materials just at one click.**

Splunk SPLK-3003 Core Consultant Certification Details:

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
Books / Training	**Services: Core Implementation**
Schedule Exam	**Pearson VUE**
Sample Questions	**Splunk Core Consultant Sample Questions**
Practice Exam	**Splunk SPLK-3003 Certification Practice Exam**

Splunk SPLK-3003 Syllabus:

Topic	Details	Weights
Deploying Splunk	- Define Splunk Validated Architectures (SVA) - Articulate how and why Splunk grows from standalone environment to distributed environment with indexer and search head clustering - Explain the difference between high availability and disaster recovery and how both can be addressed in Splunk	5%

Topic	Details	Weights
Monitoring Console	- Describe which instances are suitable to configure as the Monitoring Console - Articulate how to configure the MC for a single or distributed environment - Examine how the MC uses the server roles and groups - Describe how MC health checks are performed and can be extended	8%
Access and Roles	- Identify authentication methods - Describe LDAP concepts and configuration - List SAML and SSO options - Define roles and articulate how roles are used to secure data	8%
Data Collection	- Articulate the different ways data can be ingested by an indexer - Articulate how one Splunk instance communicates with another Splunk instance (S2S) - Describe the types and configuration of data inputs - Describe ways to troubleshoot data inputs	15%
Indexing	- List indexing artifacts and locations - Describe event processing and data pipelines - Describe the underlying text parsing and indexing process - List data retention controls	14%
Search	- Describe how to use search job inspection; explain the inner-workings of a search - List the different search types - Describe how to maximize search efficiency - Describe how sub-searches work	14%
Configuration Management	- Describe a deployment app - Articulate how a deployment server works - Describe deployment system configuration - Articulate how to manage deployment server	8%
Indexer Clustering	- Describe deployment and component configuration - Describe the life cycle of data using buckets - Determine failure modes and recovery processes - Articulate how multi-site clustering works - List migration procedures	18%
Search Head Clustering	- Articulate how to manage and deploy a search head cluster	10%

Topic	Details	Weights
	- Determine when a search head cluster may be needed and when a search head cluster would not be recommended - Describe content management using the deployer - Describe the role of the cluster members and the Captain - Articulate how captain election works (RAFT)	

Broaden Your Knowledge with Splunk SPLK-3003 Sample Questions:

Question: 1

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: 2

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: 3

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: 4

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: 5

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

Question: 6

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: 7

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: 8

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: 9

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: 10

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

Avail the Study Guide to Pass Splunk SPLK-3003 Core Consultant Exam:

- Find out about the SPLK-3003 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-3003 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 Consultant 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-3003 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. SPLK-3003 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-3003 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.