SPLUNK SPLK-3001 STUDY GUIDE PDF

Grab the Splunk Enterprise Security Admin Certification PDF Questions & Answers

Details of the Exam-Syllabus-Questions

SPLK-3001

Splunk Enterprise Security Certified Administrator

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

www.CertFun.com

Table of Contents:

Get an Overview of the SPLK-3001 Certification:

Who should take the **SPLK-3001 exam**? This is the first question that comes to a candidate's mind when preparing for the Enterprise Security Admin certification. The SPLK-3001 certification is suitable for candidates who are keen to earn knowledge on the Enterprise and grab their Splunk Enterprise Security Certified Administrator. When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But SPLK-3001 study guide PDF is here to solve the problem. SPLK-3001 PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the Splunk SPLK-3001 Certification?

There are several reasons why one should grab the SPLK-3001 certification.

- The Enterprise Security 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 Security Certified Administrator** is a powerful qualification for a prosperous career.

What Is the Splunk SPLK-3001 Enterprise Security Admin Certification Exam Structure?

Exam Name	Splunk Enterprise Security Certified Administrator
Exam Code	SPLK-3001
Exam Price	$130 (USD)
Duration	60 mins
Number of Questions	61
Passing Score	700 / 1000
Schedule Exam	**Pearson VUE**
Sample Questions	**Splunk Enterprise Security Admin Sample Questions**
Practice Exam	**Splunk SPLK-3001 Certification Practice Exam**

Enhance Knowledge with SPLK-3001 Sample Questions:

Question: 1

Adaptive response action history is stored in which index?

a) modular_history
b) cim_modactions
c) cim_adaptiveactions
d) modular_action_history

Answer: b

Question: 2

How is it possible to specify an alternate location for accelerated storage?

a) Configure storage optimization settings for the index.
b) Use the tstatsHomePath Setting in indexes, conf
c) Update the Home Path setting in indexes, conf
d) Use the tstatsHomePath setting in props, conf

Answer: d

Question: 3

In order for ES to automatically take an action upon locating a particular event, what can a correlation search be configured to execute?

a) Action script
b) Activation prompt
c) Adaptive response
d) Integration script

Answer: c

Question: 4

Who can delete an investigation?

a) ess_admin users only.
b) The investigation owner only.
c) The investigation owner and ess-admin.
d) The investigation owner and collaborators.

Answer: a

Question: 5

To which of the following should the ES application be uploaded?

a) The indexer.
b) The KV Store.
c) The dedicated forwarder.
d) The search head.

Answer: d

Question: 6

What are the steps to add a new column to the Notable Event table in the Incident Review dashboard?

a) Configure -> Incident Management -> Notable Event Statuses
b) Configure -> Content Management -> Type: Correlation Search
c) Configure -> Incident Management -> Incident Review Settings -> Event Management
d) Configure -> Incident Management -> Incident Review Settings -> Table Attributes

Answer: c

Question: 7

When is it appropriate to use Auto Deployment on Splunk_TA_ForIndexers in a distributed search configuration?

a) When the indexers are clustered.
b) When there are multiple indexers with the same retention settings.
c) When there are multiple indexers with different volume and retention settings.
d) When there are multiple indexers with the same storage volume settings.

Answer: d

Question: 8

After data is ingested, which data management step is essential to ensure raw data can be accelerated by a Data Model and used by ES?

a) Extracting Fields.
b) Normalization to the Splunk Common Information Model.
c) Normalization to Customer Standard.
d) Applying Tags.

Answer: b

Question: 9

Which of the following is a way to test for a property normalized data model?

a) Use Audit -> Normalization Audit and check the Errors panel.
b) Run a | datamodel search, compare results to the CIM documentation for the datamodel.
c) Run a | loadjob search, look at tag values and compare them to known tags based on the encoding.
d) Run a | datamodel search and compare the results to the list of data models in the ES normalization guide.

Answer: b

Question: 10

When creating a correlation search, which command will generate a notable event if the risk score for any one host is greater than 100?

a) | where 'risk_score' > 100
b) | eval risk_score > 100
c) | sum(host)risk_score > 100
d) | All_Risk.risk_score > 100

Answer: a

What Study Guide Works Best in Acing the Splunk SPLK-3001 Enterprise Security Admin Certification?

The SPLK-3001 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 Security 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-3001 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-3001 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-3001 practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven SPLK-3001 Practice Test for Success!!!

Do you want to pass the SPLK-3001 exam on your first attempt? Stop worrying; we, CertFun.com are here to provide you the best experience during your Splunk Enterprise Security Certified Admin preparation. Try out our free mock tests to get a glimpse of our quality study materials, and build your confidence with the premium **SPLK-3001 practice tests**. Our expert-designed questions help you to improve performance and pass the exam on your first attempt.